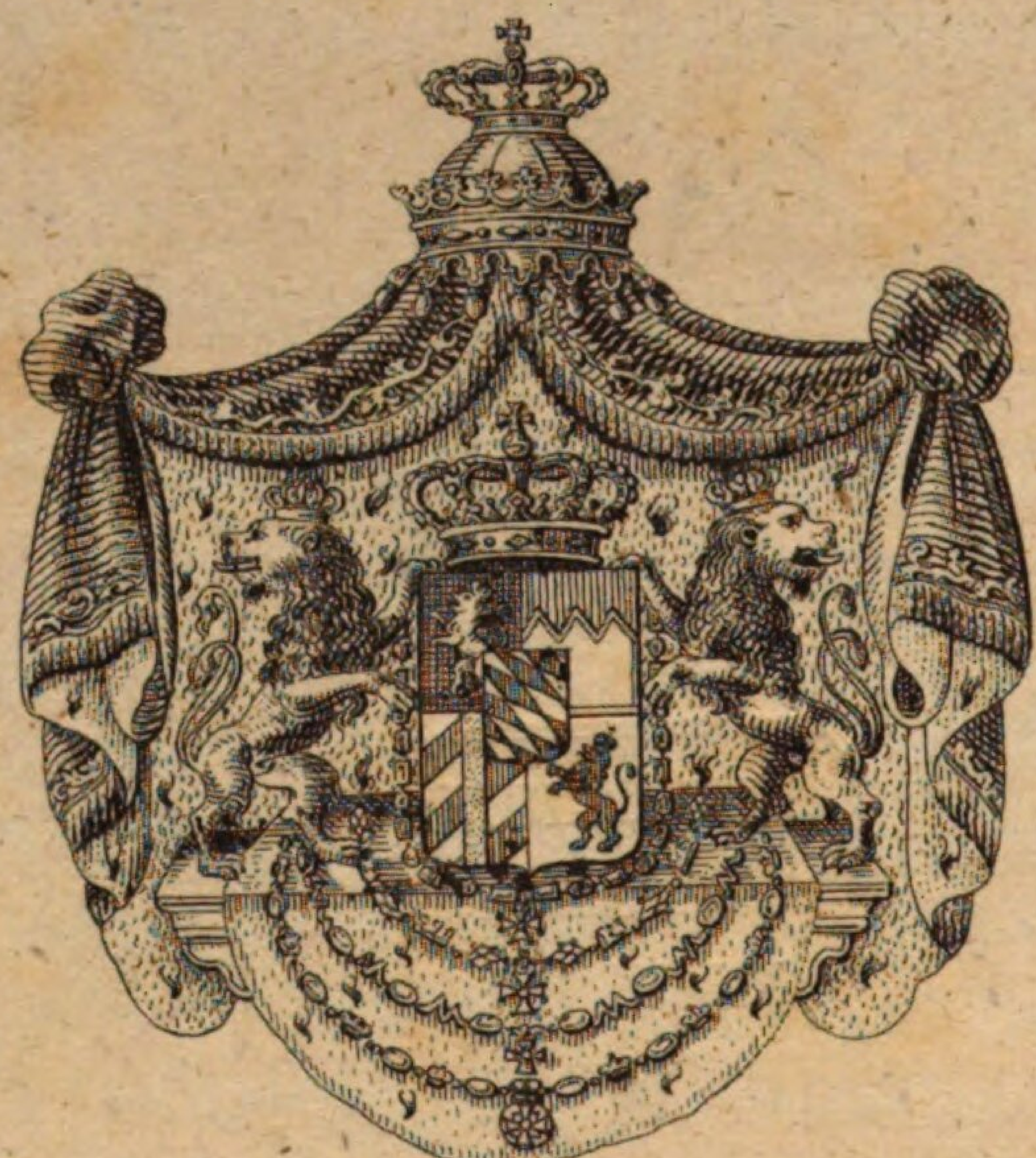
4° Mat. un 16 l - 1 Crelle



BIBLIOTHECA
REGIA
MONACENSIS.

<36640588320011

<36640588320011

Bayer. Staatsbibliothek

Encyklopädische Darstellung
der
Theorie der Zahlen
und
einiger anderer damit in Verbindung stehender analytischer Gegenstände;

zur Beförderung und allgemeineren Verbreitung

des Studiums der Zahlenlehre durch den öffentlichen und Selbst-Unterricht

elementar und leicht faſslich vorgetragen

von

A. L. Crelle,

Königlich-Preuſsischem Geheimen-Ober-Baurathe, Mitgliede der Königlichen Akademie der Wissenschaften zu Berlin, Correspondenten der Kaiserlichen Akademie der Wissenschaften zu St. Petersburg und der Königlichen Akademieen der Wissenschaften zu Neapel und Brüssel, auswärtigem Mitgliede der Königlichen Akademie der Wissenschaften zu Stockholm, Ehrenmitgliede der Hamburger Gesellschaft zur Verbreitung der mathematischen Wissenschaften.

Erster Band.

(Besonders abgedruckt aus dessen „Journal für die reine und angewandte Mathematik, Bd. XXVII, XXVIII und XXIX.")

Berlin,
Druck und Verlag von G. Reimer.
1845.

302. a.

BIBLIOTHECA
REGIA
MONACENSIS

Vorrede.

Die reine Mathematik hat drei wesentlich verschiedene Theile. Der erste Theil, die *Rechenkunst*, geht von dem Begriff der Zahl aus und zerfällt gewöhnlich weiter in Arithmetik, Algebra, Differential-, Integral- und Variationsrechnung. Der zweite Theil, die *Geometrie*, hat Figuren im Raume zum Gegenstande. Der dritte Theil, die *Mechanik*, beschäftigt sich mit den Gesetzen des Gleichgewichts und der Bewegung der Körper: die *Statik* mit dem *Gleichgewicht* fester Körper, die Hydrostatik mit dem Gleichgewicht flüssiger Körper, die *Dynamik* mit der *Bewegung* fester Körper und die *Hydrodynamik* mit der *Bewegung* flüssiger Körper.

Von mehreren Naturwissenschaften, in welchen die reine Mathematik besonders viele Anwendungen findet, z. B. von der Sternkunde, der Lehre vom Licht, von der Wärme, von der Zeitmessung, von der Gestalt der Erde u. s. w., also von Astronomie, Optik, Wärmelehre, Chronologie, Geographie u. s. w. pflegt man auch die Gesammtheit *angewandte Mathematik* zu nennen. Diese letztere Benennung ist, so scheint es, nicht ganz passend; denn wären jene Zweige des Wissens *Mathematik*, so müfste man auch die gesammte Physik, die Technik, ja fast alle andern Wissenschaften von den sinnlichen Dingen ebenfalls angewandte *Mathematik* nennen, weil sie *alle* Gebrauch von der Mathematik machen; was aber nicht und mit Recht nicht geschieht, indem die Mathematik ihnen nur Hülfe leistet und ihr mathematischer Theil mehr oder weniger der *kleinere* ist. Es dürfte also alles Jenes nur *Anwendungen* der Mathematik zu nennen, nicht unter dem Namen *angewandte Mathematik* zur Mathematik selbst zu zählen sein. Die sogenannte *reine* Mathematik sollte ausschliefslich Mathematik heifsen.

Gegentheils erklären Einige den obigen dritten Theil der reinen Mathematik, die Mechanik, nicht für *reine*, sondern schon für *angewandte* Mathematik, weil sie von der Rechenkunst und Geometrie *Anwendungen* auf die Gesetze des Gleichgewichts und der Bewegung mache. Aber auch dieses scheint nicht ganz angemessen und consequent, sondern vielmehr nur eine Art von Verwechselung der Mechanik mit der Maschinenlehre und mit einzelnen Theilen der Physik zu sein. Die eigentliche Mechanik oder die Lehre von den Gesetzen des Gleichgewichts und der Bewegung ist gewifs *völlig reine* Mathematik, obgleich sie Anwendungen von der Rechenkunst und der Geometrie macht, diese beiden mit dem eigenthümlichen Begriffe von *Kraft* verbindend. Wollte man die Mechanik jener Anwendungen wegen *nicht* zur reinen, sondern zur angewandten Mathematik zählen, so müfste man consequenterweise gleiches auch mit der Geometrie thun; denn auch sie macht schon *Anwendungen* von der Rechenkunst und verbindet dieselbe mit dem eigenthümlichen Begriffe von der *Gestalt*. Alsdann würde die Rechenkunst *allein* für die reine Mathematik übrig bleiben, Sie darauf zu beschränken, wäre aber wieder nicht richtig. Denn ganz ebenso abstract, wie der Begriff von der *Zahl* ist, dessen Abgezogenheit von der sinnlichen Wahrnehmung die Wissenschaft von der Zahl, die Rechenkunst, zu einer reinen oder abstracten Wissenschaft macht: eben so abstract ist auch der Begriff von der *Gestalt* und derjenige von der *Kraft*.

Die reine Mathematik, oder schlechthin die Mathematik, hat also in der That wesentlich *drei* Theile; nicht mehr und nicht weniger: *Erstlich* die Rechenkunst, die blofs von dem Begriffe der Zahl ausgeht; *zweitens* die Geometrie, welche von den Begriffen der Zahl und der Gestalt ausgeht, und *drittens* die Mechanik, welche von den Begriffen der Zahl, der Gestalt und der Kraft anhebt.

Diese allgemeinen Bemerkungen mögen hier bei der Gelegenheit stehen, wo der Gegenstand Dessen was hier folgt aus der Gesammtheit der mathematischen Erkenntnisse auszuheben war.

Die *Theorie der Zahlen*, nemlich die Lehre von den Eigenschaften der *ganzen* Zahlen und von ihren Verbindungen mit einander, gehört in den *ersten* Theil der Mathematik, in die *Rechenkunst*; aber keineswegs in die *Arithmetik* oder in die Lehre vom Rechnen mit bestimmten Zahlen insbesondere; denn sie nimmt auch die Algebra und selbst die Differential- und Integral-Rechnung zu Hülfe, während sie, rückwärts, nicht blofs der Arithmetik, sondern auch der Algebra und der Differential- und Inte-

gral-Rechnung wiederum Hülfe leistet. Die Benennung *höhere Arithmetik*, welche man zuweilen der Theorie der Zahlen giebt, ist also nicht ganz passend. Jener Theil der Rechenkunst wird immer am angemessensten *Theorie der Zahlen* oder *Zahlenlehre* heifsen.

Diese Theorie der Zahlen ist nun, wenigstens in ihrer weitern Ausdehnung, ein *neuerer* Theil der Mathematik; etwa wie die Differential- und Integral-Rechnung. Bei den Alten finden sich nur erst Spuren davon. Erst etwa mit *Fermat* begann ihre Entwickelung, und zu ihrer jetzigen Ausdehnung gelangte sie erst in noch neuerer Zeit; vorzüglich durch *Euler*, *Lagrange*, *Gaufs*, *Legendre*; später durch *Jacobi*, *Dirichlet* u. s. w. So neu sie aber ist, hat sie doch schon einen ungemeinen Aufschwung gewonnen. Sie ist schon zu einer grofsen Masse von Sätzen angewachsen, und erweitert sich täglich.

Obgleich aber neu, ist es bei dieser Theorie eine auffallende Erscheinung, dafs bis jetzt noch so ungemein wenig davon *allgemeiner* bekannt und *verbreitet* worden ist. Die Differential- und Integralrechnung, wiewohl eigentlich doch noch jünger als die Theorie der Zahlen, ist schon bei weitem allgemeiner gekannt. Es giebt schon eine Menge, selbst ganz elementarer Lehrbegriffe derselben, während von der Theorie der Zahlen eigentlich noch *kein einziges* elementares Lehrbuch existirt, welches sich darüber einigermafsen weiter verbreitete. Alles, was von der Theorie der Zahlen zur *allgemeineren* Kenntnifs gelangt ist, beschränkt sich fast nur auf das Wenige, was die Lehrbücher der Mathematik von einigen Eigenschaften der Zahlen rücksichtlich ihrer Theilbarkeit, von den gröfsten gemeinschaftlichen Theilern, von den Kettenbrüchen und von der Auflösung der Gleichungen ersten Grades zwischen zwei ganzen Zahlen, unbestimmte Analytik genannt, zu geben pflegen. Und auch diese sogenannte unbestimmte Analytik geben öfters die Lehrbücher, sogar innerhalb des sehr beschränkten Umfanges, in welchem sie davon handeln, nur sehr unvollkommen und wenig genügend.

Diese Erscheinung des Zurückbleibens der allgemeineren Verbreitung der Theorie der Zahlen läfst sich vielleicht daraus erklären, dafs diese Theorie beim ersten Anblick weniger, wie man es nennt, *gemeinnützig* zu sein scheint, als z. B. die Differential- und Integralrechnung. Unter Gemeinnützigkeit versteht man Brauchbarkeit zu Anwendungen im gemeinen Leben. Auch mag ein Grund des Zurückbleibens der sein, dafs, wie es gewöhnlich bei den *Entdeckungen* der Fall ist, die ersten Wege

zu den verschiedenen neuen Wahrheiten nicht immer die geradesten und hellsten waren und der Vortrag der neuen Wahrheiten auf solchen Wegen, und auch wohl später auf den besseren Wegen, wenig allgemein verständlich ausfiel, weil die Entdecker nur die Absicht hatten, Das was sie fanden überhaupt nur erst mitzutheilen, den Lernenden es überlassend, sich den Vortrag nach ihren Bedürfnissen selbst deutlicher zu machen.

Was nun aber den *wahren Nutzen* der Theorie der Zahlen betrifft, so ist es unbillig, ihn geringer anzuschlagen, als den anderer Theile der Mathematik; denn es ist überhaupt unrichtig, den eigentlichen Nutzen der Mathematik etwa nur, oder auch nur vorzugsweise in der Brauchbarkeit ihrer Sätze zu *Anwendungen* im gemeinen Leben zu suchen und ihn nach dieser Brauchbarkeit *insbesondere* abzumessen. Um dieses zu erörtern, wird der Nutzen der Mathematik etwas näher zu betrachten sein.

Derselbe ist *zwiefach.*

Erstlich findet die Mathematik fast in allen Naturwissenschaften, ja selbst beinahe in allen Theilen der menschlichen Erkenntnisse, wenigstens derjenigen von den sinnlichen Dingen, als Hülfswissenschaft *Anwendung* und ist für dieselben mehr oder weniger unentbehrlich; letzteres namentlich in der Wissenschaft von den Himmelskörpern und dem Erdkörper und deren Bewegung; in der gesammten Physik, die Chemie mit eingeschlossen; in der gesammten Technik, in ihrem weitesten Umfange; selbst in den Staatswissenschaften; so wie endlich bei unzähligen Verhältnissen und Begegnissen des gemeinen Lebens. Von einigen jener Wissenschaften macht sie sogar einen fast überwiegenden Theil aus, z. B. von der Astronomie, der Optik u. s. w.

Zweitens ist die Mathematik ganz vorzüglich geeignet, *das Denkvermögen zu entwickeln* und zu üben: denn da sie es nur mit *unbestreitbaren* Wahrheiten zu thun hat, so übt sie den Verstand im *sichern* Schliefsen und gewöhnt ihn, nur Das als wahr anzuerkennen, was sich *beweisen* läfst. Sie ist eines der kräftigsten Heil- und Vorbeugungsmittel gegen den Irrthum und eine treffliche Gymnastik für den menschlichen Geist.

Der Nutzen der Mathematik ist also keineswegs auf ihre Brauchbarkeit zu *Anwendungen* im gemeinen Leben *allein* beschränkt, sondern sie hat schon *an und für sich selbst,* als Gegenstand für die Entwickelung der Denkkraft, *unabhängig von jeder Anwendung* Nutzen; und zwar sehr grofsen Nutzen. Als Hülfswissenschaft ist sie nur für Diejenigen mehr oder weniger nützlich, welche einer solchen Hülfe für

ihr besonderes Streben und Treiben bedürfen: als Gymnastik des Verstandes dagegen ist sie für *Jeden ohne alle Ausnahme,* der Anspruch auf Civilisation macht, förderlich und nothwendig. Dieses wird auch in gewissem Maafse anerkannt; denn man lehrt in den Schulen *mit Recht Jedem* Mathematik in einem gewissen Umfange, ohne danach zu fragen, welcherlei *Anwendung* er davon in seinem künftigen Lebensberufe zu machen haben werde.

Die Gröfse der beiden Arten des Nutzens der Mathematik gegen einander abzuwägen würde keinen rechten Zweck haben, indem *alles* Nützliche gut und schätzbar und es nicht entscheidend ist, welches davon es mehr oder weniger sei. Aber Das ist zu bemerken, dafs der Nutzen der Mathematik als Übungsmittel der Denkkraft *unzweifelhaft* und *unfehlbar* ist und dafs man in dieser Benutzung nicht leicht zu weit gehen kann, während es sich mit dem andern Nutzen, demjenigen der Anwendungen im gemeinen Leben und selbst in andern Erfahrungs-Wissenschaften, nicht ganz eben so verhält. Diese Bemerkung ist nöthig, damit um so weniger die *Anwendungen* allein, oder auch nur dieselben *vorzugsweise* als *Zweck* der Mathematik betrachtet und ihre Pflege etwa nur nach dem *Bedürfnifs* jener Anwendungen abgemessen werden zu müssen scheinen möge. In der Entwickelung und Übung seiner Denkkraft kann offenbar Niemand so leicht zu weit gehen; und der Nutzen, welchen ihm die Mathematik dabei leistet, ist unzweifelhaft: bei den Anwendungen auf sinnliche Dinge dagegen ist viele *Vorsicht* nöthig; denn in demselben Maafse, wie die Voraussetzungen bei den Dingen und den Erscheinungen, auf welche die Mathematik angewendet wird, unsicher und vielleicht unrichtig sind, sind auch die Resultate, zu welchen man durch die Anwendungen gelangt, ebenfalls, und zwar ganz unfehlbar und nothwendig unsicher und unrichtig; *eben* aus dem Grunde, weil der mathematische Weg, der von den Voraussetzungen zu den Resultaten führt, *nicht* trügt und folglich Das, was an den Voraussetzungen mangelhaft war, unabwendlich auf die Resultate Einflufs haben *mufs.* Verläfst man sich auf die Resultate, in der Meinung, dafs ja die unfehlbare Mathematik zu ihnen führte, zu sehr, so kann es kommen, dafs durch Anwendungen der Mathematik das beabsichtigte Ziel nicht erreicht wird, dafs man statt Wahrheiten Irrthümer findet und dafs man so durch die Mathematik statt zu Nutzen zu Schaden gelangt. Es giebt nur wenige Dinge, bei welchen die Voraussetzungen so sicher sind und die Natur-Gesetze, von welchen man ausgeht, so isolirt wirken, dafs man wirklich der Richtigkeit der Resultate der Anwendungen der Mathe-

matik versichert sein kann. Es ist dies beinahe nur allein bei der Bewegung der Himmelskörper und bei der des Lichts (also in der Astronomie und Optik) der Fall. In allen andern Theilen der Physik, ferner fast in der gesammten Technik und wo sonst die Mathematik zur Anwendung kommen mag, sind entweder die Voraussetzungen, von welchen man ausgeht, zweifelhaft, oder sie werden so sehr durch andere Wirkungen modificirt, oder stehen mit andern Wirkungen, die man noch nicht kennt, oder die zu complicirt sind, als dafs sie sich in Betracht ziehen liefsen, so vielseitig in Verbindung, dafs diejenigen Voraussetzungen, auf welche man fufst, und die Resultate, welche man findet, sehr wohl irrig sein können. Freilich ist es wahr, dafs die *elementaren* und die *einfachen* Sätze der Mathematik, der Geometrie und Mechanik sowohl, als der Rechnung, *überall* und fast jeden Augenblick, in allen möglichen Lebensverhältnissen zur Anwendung kommen, und dafs also jene Sätze für die Anwendung durchaus nothwendig und völlig unentbehrlich und von dem weit umfassendsten Nutzen sind. Allein in diesen *gewöhnlichen* Fällen, wo man von schon *complicirtem Gegebenen* ausgeht, ist es auch leichter, den Fehler zu entdecken, wenn die Resultate nicht passend ausfallen. Es zeigt sich sogleich, dafs, und wo Fehler in den *Voraussetzungen* liegen. Anders ist es, wenn man von der Mathematik verlangt, sie solle helfen, tiefer in die Natur der Dinge zu dringen und das Mittel sein, von *einfachen* Naturgesetzen an, die an sich selbst auch vollkommen richtig erkannt sein mögen, zu complicirten Resultaten zu gelangen. Hier können wegen *übergangener* Voraussetzungen, welche modificirend mitwirken, grofse Irrthümer die Folge sein, und man kann sogar, von der Richtigkeit und Unfehlbarkeit der mathematischen Sätze und vielleicht auch von der Richtigkeit der vereinzelten Voraussetzungen an sich, wo sie Statt findet, bestochen, verleitet werden, das Unrichtige für das Wahre zu *halten;* und daraus kann in mannigfaltigen Lebens-Verhältnissen sogar unmittelbarer und bedeutender *Nachtheil* entstehen. Die Technik z. B. liefert zahlreiche Beispiele, wo dergleichen Schäden wirklich erfolgten. Auch in andern Dingen fehlen Beispiele seltsamer Irrthümer nicht. Wurde nicht z. B., um nur Eins und etwas Pikantes zu nennen, *Malthus,* wie es beinahe scheint, insbesondere durch die Achtung für einige mathematische Sätze von den arithmetischen und geometrischen Reihen dazu verleitet, zu schliefsen, es sei dringend nöthig, die Fortpflanzung und Vermehrung des menschlichen Geschlechts zu hemmen und zu beschränken, weil sonst der Menschen so viele werden könnten, dafs sie nicht mehr auf der Erde Nahrung finden

würden! Hätte *Malthus* die *Voraussetzungen*, auf welche er seine Rechnungen gründete, nur ein klein wenig verändert, so würde er *Anderes* gefunden haben. Man darf also den Nutzen der Mathematik für *Anwendungen* ja nicht allzuhoch anschlagen. Am wenigsten darf man ihn für den *einzigen* Nutzen, welchen diese Wissenschaft haben kann, und auch nicht für den vorzüglichern halten. Man darf indessen auch wiederum nicht etwa, wenn man wiederholt gewahr wird, wie oft die Mathematik in ihren Anwendungen zu unrichtigen Resultaten führt, die Schuld davon auf *sie* werfen, und nicht schliefsen, sie sei überhaupt wenig nütze und verdiene kein angelegentliches Studium und keine weitere Entwickelung, weil sie, zu Anwendungen im gemeinen Leben benutzt, so oft zu Irrthümern verleite: die Schuld liegt gewifs nicht an der Mathematik, sondern an der *Art* ihrer Anwendung; das *Werkzeug* ist gut, sicher und werthvoll, aber es kommt auf die richtige *Handhabung* desselben an. Die Anwendungen der Mathematik im weitern Umfange auf complicirte Fälle des gemeinen Lebens, wenn man bei denselben von abstracten Erfahrungssätzen ausgeht, sind mifslich und erfordern immer Vorsicht: aber gerade der *andere* Theil des Nutzens der Mathematik, bei der Übung und Entwickelung der Denkkraft, ist es nun wieder, der die Mifslichkeit hebt und der zur Anleitung zu der nöthigen Vorsicht verhilft. Die Benutzung der Mathematik zur Übung des Denkvermögens darf nur erst vorhergehen, so folgt der andere Nutzen für Anwendungen, der dann, und *nur* dann nicht minder grofs und weit umfassend sein wird, mit gröfserer Sicherheit von selbst. Wenn erst durch fleifsige Übung des *Urtheils vermittels der Mathematik* (ohne Rücksicht auf Anwendungen) ein mathematischer *Geist* geweckt worden ist, und nur dann erst, kann man auch dreister auf den Nutzen der Mathematik bei den Anwendungen rechnen. Das blofse *Wissen* in der Mathematik, auf *Anwendungen* berechnet, die Bekanntschaft mit dazu dienenden Sätzen und Formeln, selbst mit dem Mechanismus, der zu solchen Sätzen führt, ist zu richtigen Anwendungen noch nicht hinreichend, sondern der mathetische *Geist*, oder die mathematische *Art zu denken* mufs der Leitfaden sein. Erst wer *damit* an die Anwendungen geht, wird weniger leicht irren; denn er wird vor Allem erst untersuchen, *was* eigentlich die Mathematik zu leisten vermöge und wo und auf welche Weise das Werkzeug mit Nutzen zu gebrauchen sei. Denjenigen, welche eine weiter ausgeführte wissenschaftliche Entwickelung erlangt haben, wird jener mathematische Geist mehr oder weniger eigen geworden sein, und daher sind auch unpassende Anwendungen der Mathematik in den mehr wissenschaftlich ausge-

bildeten Theilen der menschlichen Erkenntnisse, wie z. B. in der Physik, in den Staatswissenschaften u. s. w., weniger zu fürchten. Wohl aber haben sie Diejenigen zu fürchten, welche ihre eigentlich geistige Entwickelung oder wissenschaftliche Bildung weniger beendigten und früher zu unmittelbarer practischer Lebensthätigkeit übergingen, und die sich dann der Mathematik als Werkzeug bedienen, z. B. Techniker aller Art, oder Andere, welche verwickeltere Rechnungen auszuführen haben; ja selbst Alle, die im Leben nach zusammengesetzten Schlufsfolgen, wäre es auch nur nach den Gesetzen der Wahrscheinlichkeit, zu handeln haben, u. s. w. Daher ist es denn *ganz recht*, dafs die Mathematik so viel als möglich in den Schulen, selbst in denen, welche den nicht eigentlich Gelehrten ihre Vorbereitung geben, zuerst *ohne* alle Rücksicht auf Anwendungen im gemeinen Leben geübt werde: nicht sowohl zu dem Zwecke, dem Lernenden mathematisches *Wissen* für Anwendungen beizubringen, als vielmehr, um ihn an die mathematische *Art zu urtheilen* zu gewöhnen und den mathematischen *Geist* in ihm zu wecken.

Zu dieser Übung und also zur Erzielung des davon zu erwartenden Nutzens ist nun aus den verschiedenen Theilen der reinen Mathematik auch die *Theorie der Zahlen* ganz vorzüglich geeignet: wenn nicht mehr, so doch wenigstens eben so sehr, als die Elemente der sonstigen Rechenkunst und der Geometrie und Mechanik, die man auch in den Schulen allgemein zu lehren pflegt (wenigstens jene, die Elemente der *Rechenkunst* und der *Geometrie*, während häufig die Elemente der *Mechanik*, die doch, selbst schon zu Anwendungen im gemeinen Leben gewifs eben so nützlich sind, als die der Rechenkunst und Geometrie, wohl mit Unrecht zurückbleiben). Auffallend ist es daher, dafs, während die Wiederholung des Vortrages der Elemente der Rechenkunst und Geometrie in immer neuen Lehrbüchern ohne Ende und bis zum äufsersten Überflufs fortwährt, für die Benutzung der Theorie der Zahlen fast gar nichts geschieht. Es wäre in der That wohl zu wünschen, dafs es anders wäre. Zwar liefert die Theorie der Zahlen wieder weniger für unmittelbare *Anwendungen* Taugliches, als die übrigen Elemente der Mathematik, aber desto mehr ist sie geschickt *zur Übung und Entwickelung des Urtheilsvermögens.*

Das Letztere kommt *daher*, dafs einestheils die für die Theorie der Zahlen nöthigen Schlüsse ungemein mannigfaltig sind und dafs diese Theorie der Denkkraft einen besonders freien Spielraum eröffnet und sie weniger, wie z. B. die Algebra und die Differential- und Integralrechnung, in einen bestimmten Algorithmus einzwängt:

anderntheils aber von dem eigenthümlichen Umstande, dafs wohl kein Theil der Mathematik mit so *unbedingten* Wahrheiten umgeht, wie die Theorie der Zahlen. Allerdings sind freilich auch die Schlüsse und Sätze der übrigen Mathematik vollkommen wahr und unzweifelhaft, aber doch nur von den Axiomen und Postulaten an; und jeder andere Theil der Mathematik hat deren. Wer hier über die Axiome Rechenschaft verlangt, verleitet sich, an Allem zu zweifeln, was daraus folgt; eben darum, weil es unzweifelhaft *folgt.* Wer das eilfte Axiom des Euklides nicht zugeben will; wer von der Ebene einen bestimmteren mathematischen Begriff verlangt, als ihn die Elemente zu geben pflegen; wer das Axiom, die krumme Linie sei länger, als die gerade zwischen ihren Endpuncten, nicht annimmt, der darf auch an den Resultaten der gesammten Geometrie zweifeln, wenn ihm anders nicht die Erfahrung a posteriori genügt, dafs kein Resultat dem andern widerspricht. Wer im Calcul an dem axiomatischen Übergange vom Rationalen zum Irrationalen, vom Stetigen zum Unstetigen u. s. w. Anstofs nimmt, darf auch an den Resultaten der Rechenkunst Anstofs nehmen. Wer in der Mechanik von den Axiomen der Beharrung, der Geradlinigkeit der ungestörten Bewegung, vom Parallelogramm der Kräfte u. s. w. erschöpfende Beweise verlangt, kann auch die sämmtlichen Resultate der Mechanik für nicht hinreichend begründet erachten. Überall sind diese Theile der Mathematik erst *nur von da an,* wo sie aus dem unerforschten und unerforschlichen Unendlichen in das Gebiet des Sinnlichen, Endlichen hervorgetreten sind, *vollkommen* sicher. Die Theorie der Zahlen hingegen hat keine Axiome und bedarf ihrer nicht, wenn man nicht etwa über den Begriff der Zahl selbst grübeln will; was aber nichts weiter als *Absicht* des Zweifelns sein würde. Die Theorie der Zahlen liegt *ganz* im Bereiche des Endlichen und Sinnlichen; wenigstens in so weit sie nicht andere, mit Axiomen in Berührung kommende Theile des Calculs zu Hülfe nimmt. Daher sind denn auch ihre Sätze *vollkommen* gewifs, und daher ist sie *ganz vorzüglich* zur Übung der Urtheilskraft und recht eigentlich des *practischen* Denkens, wenn der Ausdruck erlaubt ist, desjenigen Denkens, welches in seinem wahren Bereiche, im Bereich des Endlichen bleibt, geschickt. Wenn irgend etwas in dem gesammten Umfange des menschlichen Wissens *vollkommen* wahr und sicher ist, so ist es die *Theorie der Zahlen.*

Aus diesen Erwägungen geht nun hervor, dafs es vielleicht ein nützliches Bemühen sein dürfte, zu versuchen, ob sich nicht dazu beitragen lasse, die Theorie der Zahlen mehr zum *Gemeingut* zu machen; und von diesem Bemühen geht die

hier folgende Sammlung von Sätzen aus. Ihrer Einrichtung und Anordnung liegen folgende Betrachtungen zum Grunde.

Damit Wahrheiten, deren Erkenntnifs die Urtheilskraft in Anspruch nimmt, recht *Vielen* von verschiedener Fassungskraft, und selbst Personen im jugendlichen Alter zugänglich werden mögen, dürfte es vor Allem nöthig sein, sie *so* auseinander zu setzen, dafs das Urtheil bei den Sätzen und ihren Beweisen nur *Schritt um Schritt* dem Vortrage folgen darf, um zum Ziele zu gelangen. Alle *einfachen* Schlufsfolgen müssen, scheint es, angegeben, keine darf übersprungen werden; denn zu sagen, *welche* Schlufsfolgen und *wie* sie an einander zu fügen sind, oder fehlende zu ergänzen, kann nicht eine Aufgabe für den Schüler sein, da selbst öfters über das Erste die Lehrer nicht einig sind und das Rechte und Beste verfehlen können; wie es schon der Umstand zu erkennen giebt, dafs gar viele *Verschiedenheit* in der Anordnung und Aufeinanderfolge der Sätze und in der Art und Anordnung der Beweise möglich ist. Nach meiner Meinung ist die heuristische Methode für den *ersten* Unterricht in der Mathematik nur mit grofser Einschränkung passend. Der Schüler kann unmöglich, wären auch seine Kräfte noch so bedeutend, eher urtheilen und *selbst* finden, ehe er nicht wenigstens durch *einigen* Vorrath von *Einsichten* dazu ausgerüstet ist; und das gerade besonders in der Mathematik, wo nur Eins aus dem Andern folgt. Er wird immer um so besser für das Selbstfinden befähigt sein, je mehr *Material* zum Weiterschliefsen er sich schon angeeignet hat. Welche Erfolge der Mangel an *Wissen* bei Individuen haben kann, die gerade recht viele Neigung zum Selbstfinden in sich verspüren, zeigt sich z. B. an den Kreis-Quadrirern, den Parallelen-Grüblern und Andern, die sich abmühen, das Unfindbare zu suchen. Wären diese Personen mit einer hinreichenden Masse von *Wissen* ausgerüstet, so würden sie bald die Nichtigkeit und Unnützlichkeit ihrer Bemühungen einsehen und davon ablassen. Diesemnach soll die hier folgende Schrift die *Beweise* der Sätze, auf welche es in der Zahlentheorie insbesondere, und sogar mehr als auf die Sätze selbst ankommt, da vorzüglich sie zur Übung der Urtheilskraft geschickt sind, immer *vollständig* geben; und das nicht blofs im Anfange, sondern durch die ganze Schrift hindurch. Wo *mehrere* Beweise zu merken sind, werden sie gegeben werden. Man darf aber, insofern die Schrift zum Unterricht benutzt werden möchte, sei es zur Selbstbelehrung, oder zum Unterricht in den Schulen (und diese letzte Bestimmung hat sie *vorzüglich*), keinesweges etwa fürchten, dafs der Schüler durch eine derartige Darlegung der Gegen-

stände am Auswendiglernen werde gewöhnt und dem Selbstdenken und Selbstfinden entwöhnt werden. In der Schule ist dies gar nicht zu fürchten. Ist dort das Buch in der Hand des Lehrers, so bleibt es diesem überlassen, nach den Umständen und nach seinem Ermessen die Beweise ganz oder theilweise zur Aufgabe des Selbstfindens zu machen. Ist die Schrift auch zugleich in der Hand des Schülers, so darf der Lehrer den Sätzen und Beweisen nur eine andere Form geben lassen, um nach Belieben auf die mannigfachste Weise das Selbstdenken beim Schüler anzuregen. Beim Selbst-Unterricht verhält es sich ähnlich; dieser unterscheidet sich überhaupt von dem Schul-Unterricht wohl nur dadurch, dafs nächst dem Buch der Lernende selbst, so gut er es vermag, und so wie seine Einsicht sich erweitert, die Stelle des Lehrers vertritt.

Sodann wird sich das vorliegende Buch der äufsersten *Deutlichkeit,* nicht blofs durch *Vollständigkeit* der Beweise und Erörterungen, sondern auch durch die *Art* ihrer Darlegung befleifsigen. Es ist wohl um die *wahre* Deutlichkeit eine eigene Sache. Die Erreichung derselben ist, wenn man den Ausdruck gestatten will, eine *Kunst:* eine Kunst, um deren Ausbildung und *wissenschaftliche Ergründung* man sich vielleicht noch zu wenig bemüht hat, die aber gleichwohl sehr wichtig ist. Dafs die Deutlichkeit weder durch die *Weitläuftigkeit,* noch durch die *Kürze* allein zu erreichen sei, bedarf kaum der Erinnerung. Beide allein können eher Undeutlichkeit als Deutlichkeit zur Folge haben. Bestimmte, specielle Regeln für die Erzielung der Deutlichkeit möchten sich schwer geben lassen. Im Allgemeinen scheint der Weg dazu derjenige *kürzeste* Weg zu sein, welchen der Verstand vom Ausgangspuncte bis zum Ziele bei der *Überschauung* des Gegenstandes nimmt, nachdem ihm derselbe vollkommen klar geworden ist. Dafs aber die Deutlichkeit nicht immer auf dem rechten Wege zu erreichen gesucht wird, folgt schon daraus, dafs, selbst bei denjenigen mathematischen Gegenständen, die die Lehrbücher so unendlich oft abgehandelt haben, wie z. B. die Geometrie, selbst in den Büchern, die sich vorsätzlich der Deutlichkeit befleifsigen, doch immer wieder noch *andere* Wege und Darstellungsarten zum Vorschein kommen, während doch nur eine die *beste* sein kann. In diesem Puncte scheint man öfters nur fast aufs Gerathewohl oder empirisch zu verfahren; noch keineswegs, wenn man es so nennen will, *rationell,* oder auch nur mit hinreichender Bemühung um die Aufgabe. Gleichwohl wäre es anders zu wünschen. Denn der hohe, vollendete Nutzen der Mathematik, als Übungsgegenstand des Urtheils betrachtet, liegt gerade in der vollendeten Klarheit und Deutlichkeit der Einsicht und

der Überzeugung. Häufig kann Jemand einen mathematischen Satz zu verstehen *glauben*, während er doch nur erst das Ende davon nicht viel anders als gleichsam *ahndet*, oder ihn nur gleichsam wie durch einen Nebel hindurch erblickt. Die Darstellung eines mathematischen Gegenstandes, in idealer Vollendung gedacht, kann gewissermaafsen bis zur *Schönheit* sich erheben, und selbst die Sprache kann daran ihren Antheil bekommen. Eine solche Darstellung kann in ihrer Art ein geistiges *Kunstwerk* sein; und daher ist es vielleicht nicht unpassend, die Erstrebung der Deutlichkeit eine *Kunst* zu nennen. Es gehört vielleicht sogar zur Deutlichkeit des schriftlichen, eben wie des mündlichen Vortrages, ein *angebornes* Talent, was sich durch Studium schwer und vielleicht gar nicht ersetzen läfst. Man erinnere sich nur an *Euler* und *Lagrange*, die jenes Talent in hohem Grade besafsen. Was den Verfasser der vorliegenden Schrift betrifft, so fühlt er sich gewifs *sehr weit entfernt* von der Einbildung, jenes *Talent* etwa besonders zu besitzen, aber er *bemühte* sich stets um die Deutlichkeit, und er wird darnach auch hier *streben*, in so weit seine Kräfte reichen.

So nun, von der Ansicht ausgehend, dafs einmal alles nur Mögliche geschehen sollte, um den Lernenden mit der möglichsten *Leichtigkeit* auf den Standpunct der vollendeten Deutlichkeit der Einsicht zu führen, hat sich der Verfasser es hier zur Regel gemacht, nie einen Schlufs zu überspringen; während er gleichwohl sich bemühte, Alles so zusammenzudrängen und mit so wenigen *Worten* zu sagen, als es ihm möglich war. Man fürchte davon wieder nicht, es werde durch solch' einen Vortrag der Lernende zum Nachbeter und gleichsam zur Maschine werden. Zur eigenen Bewegung und zum Selbstgebrauch des Urtheils, wenn der Schüler anders dazu befähigt ist und Lust hat, bleibt demselben noch immer ein *unbegrenztes* Feld; denn die Wissenschaft ist unendlich. Und nur dadurch, dafs der Lernende erst recht viel Vorrath und Material in sich aufnimmt, wird er, wie schon bemerkt, nach der Überzeugung des Verfassers recht eigentlich zum Selbstdenken in den Stand gesetzt und angeregt werden.

Der Verfasser wird ferner überall bemüht sein, nicht sowohl dem Lernenden recht viele *Resultate* und *pikante Sätze* mitzutheilen, deren viele in der Zahlentheorie wirklich, wenigstens dem Scheine nach, an sich selbst fast nur Curiosa sind, während sie freilich in der That kostbare Samenkörner für die weitere Entwickelung darbieten: er wird vielmehr trachten, ihm die Sätze als Gegenstände aufzustellen,

an welchen *das Urtheil zu üben sei;* denn das ist, wie oben bemerkt, gerade von der Zahlentheorie insbesondere der Nutzen. In dieser Absicht, immer wieder zur Beförderung der Deutlichkeit der Einsicht, wird er auch noch folgende Mittel zu Hülfe zu nehmen suchen.

Er wird erstlich die Sätze und besonders ihre Beweise dadurch übersichtlicher und leichter zu machen suchen, daſs er sie, wo es passend scheint, in mehrere einzelne Sätze *zertheilt.* Hat man nemlich bloſs einen Hauptsatz im Auge, so sind die Beweise in der Zahlentheorie öfters sehr *lang;* das heiſst, sie bedürfen einer groſsen Menge aufeinandergefügter Schlüsse, um zum Ziele zu gelangen; wie z. B. der sogenannte Reciprocitätssatz, die Sätze von den binären und ternären Formen u. s. w. Dadurch werden solche Sätze für den Lernenden in der That *schwer;* denn was man *schwer* zu nennen pflegt, ist nichts anders, als die *Menge* und die *Vielartigkeit* der Schlüsse, die nöthig sind, um ein bestimmtes Ziel zu erreichen: an sich selbst sind die Schlüsse *einzeln* keinesweges *schwer,* sobald sie nur hinreichend in einzelne einfache Urtheile zerfället worden sind. Auch gehen bei dem ungetheilten Vortrage Sätze, die an sich auch noch andern Nutzen haben können, für diesen gleichsam verloren; wenigstens verstecken sie sich und müssen, wo sie weiter zur Benutzung vorkommen, entweder wiederholt, oder erst mühsam aufgesucht werden. Deshalb wird der Verfasser, wie gesagt, die Sätze, wo es ihm angemessen scheint, in mehrere zertheilen und, statt auf einmal, vielmehr stufenweise zu dem bestimmten Ziele fortschreiten. Es schien ihm dies die Übersicht zu erleichtern und die Deutlichkeit namhaft zu befördern.

Sodann wird er von den Beweisen, ebenfalls da wo es ihm nützlich zu sein scheint, am Schlusse eine kurze *Übersicht* geben; besonders in der Absicht, um den Lernenden auf die *Hauptpuncte* der Schluſsverbindungen aufmerksam zu machen; denn es giebt gewöhnlich bei den Beweisen bekanntlich gewisse *Haupt-Übergänge,* die gleichsam die *Nerven* der Beweise sind, und es ist besonders wichtig, daſs der Lernende sie merke.

Daſs überall die vollkommenste *Strenge* der Beweise zu erzielen gesucht werden müsse, ist offenbar; denn vorzüglich auf der vollkommensten Strenge beruht die vollendete Deutlichkeit der Einsicht. *Das Buch soll ein Übungsfeld des Denkens für Schüler sein.* Dergleichen Übungsfelder haben ohne Zweifel ihren Werth. Man erinnere sich nur an die mathematischen Werke der Alten. Bekanntlich würdigt man

mit Beifall die grofse Strenge und Consequenz bei ihren Darstellungen mathematischer Gegenstände. Man schätzt diese Auseinandersetzungen noch jetzt, nicht etwa des *Neuen* wegen, was darin jetzt nicht mehr zu finden ist, sondern ihrer logischen Schärfe und Ausgeführtheit wegen, die gerade nichts anderes als eben die *Deutlichkeit* constituiren, und durch welche sie einen guten Gegenstand zur Übung des Urtheils abgeben. Warum ahmt man bei der Behandlung der neueren Theile der Mathematik, z. B. des Calculs, den Alten nicht nach? Die gegenwärtige Schrift mag ein schwacher Versuch einer solchen Nachahmung für einen einzelnen Theil des Calculs sein.

Die äufsere *Form*, welche der Verfasser seiner Schrift gegeben hat, nemlich die Form einer blofsen *Sammlung* von Sätzen, ohne bestimmte Theilung in gröfsere und kleinere *Abschnitte*, kann sonderbar zu sein scheinen. Allein der Verfasser hatte sie zu wählen mehrere Gründe.

Zuerst nemlich ist es nach seiner Überzeugung bei dem gegenwärtigen Zustande der Zahlentheorie noch gar nicht *möglich*, ein *consequentes* System davon aufzustellen. Es sind der Lücken noch zu viele, und Das, was man besitzt, sind, so dünkt es ihm, um es gerade herauszusagen, nur Bruchstücke. Man kann zwar auf diese oder jene Weise Haupt- und Unterabtheilungen machen, aber die Anordnung wird wohl immer mehr oder weniger nur willkürlich sein; es möchte schwerlich möglich sein, einen Abschnitt consequent ganz auszufüllen, ohne in einen folgenden vorzugreifen; was doch einem guten Systeme zuwider ist.

Sodann hatte der Verfasser gar nicht die Absicht, *jeden* Lernenden, der sich seines Buches bedienen will, zu einem Kenner der gesammten Zahlentheorie zu machen, sondern er wollte nur insbesondere Jedem Materialien zur Übung seines Urtheilsvermögens darbieten. Der Lernende möge darin so weit gehen, als es ihm zusagt; oder der Lehrer möge davon auswählen, was ihm gerade angemessen scheint.

Endlich hatte der Verfasser zu der Wahl der Form seiner Schrift auch einen persönlichen Grund. Er ist nemlich, in einem jetzt schon weit vorgerückten Alter und mit einer gänzlich zerrütteten Gesundheit, der Beendigung keiner Arbeit, die er unternimmt, mehr sicher. Begann er nun eine Schrift nach irgend einem weit ausgreifenden *Systeme*, so würde jede Unterbrechung Das was fertig wurde zum Stückwerk von geringem Nutzen machen. So, wie die Schrift dagegen jetzt sein wird, schadet ihr eine Unterbrechung nichts weiter, als dafs Das, was noch kommen sollte, wenn es überhaupt etwas werth war, fehlt. Was *da* ist, behält immer seinen ver-

hältnifsmäfsigen Antheil am Zweck. Auch kann man, wenn man etwa insbesondere irgend etwas *ausheben* will, dies recht gut thun. Man darf nur die vorausgehenden Sätze, welche sich angegeben finden, aufsuchen und durchgehen; die übrigen bleiben dann zur Seite liegen.

Diesemnach gab der Verfasser seinem Buche die Form einer blofsen *Sammlung* von Sätzen, die nach keiner andern Regel geordnet sind, als nach der, *dafs kein Satz auf andere als die welche ihm vorherginyen* sich gründe. Ein Register wird eine Übersicht des Inhalts liefern. Vorausgesetzt wird in dem Buche die Kenntnifs der Arithmetik und Algebra; weiterhin auch die der übrigen Analysis. Will man ja die bezeichnete Form nicht ganz gut heifsen und die obigen Gründe dafür nicht als zureichend gelten lassen, so wird man sie doch, wenigstens in *Vergleichung* mit andern Formen, nicht *unbedingt* tadeln können, z. B. nicht in Vergleichung mit der *lexicographischen* Form, die ja noch viel weniger System im Grofsen hat.

Wie sehr bescheiden der Verfasser von seiner Arbeit denke, geht schon aus einigen der obigen Äufserungen hervor. Er will aber noch ausdrücklich bemerken, dafs er gar nicht etwa der Meinung sei, die Zahlentheorie durch die vorliegende Arbeit *erweitert* oder *bereichert* und *Neues* vorgebracht zu haben. Er hatte gar nicht die *Absicht*, danach zu streben, sondern nur die, diese Theorie möglichst recht Vielen als Gegenstand zur Übung ihrer Denkkraft darzubieten, den Vortrag danach einzurichten und die Sätze und Beweise, wiewohl in äufserster Strenge und möglichster Consequenz, für Jeden so leicht zugänglich zu machen, als es thunlich war. Ob *Neues* in seiner Arbeit sich finde, läfst er dahingestellt sein. Nach seiner Sinnesart ist es ihm gleichgültig, ob er oder ein Anderer Dieses oder Jenes gefunden habe: wenn es nur da ist. Die Freude an der Wahrheit genügt ihm. *Wahrscheinlich* wird in dem vorliegenden Buche in der That wirklich manches *Neue* zu finden sein; wenn auch weniger neue *Sätze*, so doch manche neue *Ansichten* und *Beweise*. Dies ist deshalb *wahrscheinlich*, weil der Verfasser sehr viele Beweise, und hie und da auch Sätze, wirklich *selbst* fand. Er erklärt indessen auf das bestimmteste, dafs er durchaus keinen *Anspruch* für sich auf irgend eine *Entdeckung* und auf *Priorität* macht, sondern, dafs er es im Voraus gern und willig glauben will, Dieser oder Jener habe den nemlichen Gedanken schon vor ihm gehabt.

Unter diesen Umständen, und besonders weil er so Vieles aus dem eigenen Nachdenken schöpfte, würde er denn aber auch gegenseits bei dem besten Willen

nicht im Stande gewesen sein, überall mit Sicherheit anzugeben, was Diesem oder Jenem wirklich zugehöre. Er hat es deshalb, so wie auch aus Besorgnifs, dabei Mifsgriffe zu thun, unterlassen. Blofs bei Dem, was allgemein bekannt und anerkannt ist, z. B. da, wo diese oder jene Sätze nach den Namen ihrer Entdecker *benannt* zu werden pflegen, hat er die Namen genannt. Übrigens hat er sich die Freiheit genommen, an die Ansichten, so wie an die Darstellungs- und Bezeichnungs-Art Anderer sich nicht zu binden, obgleich er, wo es nöthig war, nicht versäumte, die Correspondenz des Andern mit dem Seinigen anzuzeigen. Er ist überall, seinen Gegenstand allein im Auge, blofs seiner eigenen Überzeugung gefolgt und hat seinen Aufstellungen keine andere Stütze gegeben, als Gründe.

Berlin, im März 1845.

Inhalt des ersten Bandes.

		Seite	Nimmt Bezug auf
§. 1.	**E**rklärung und Erläuterung. Die Multiplicationszeichen betreffend. .	1.	
§. 2.	Lehrsatz. Das Product $(1+a)(1+b)(1+c) \ldots (1+n)$, entwickelt, enthält alle möglichen Producte der ν Zahlengröſsen $a, b, c, \ldots n$ zu einer, zweien, dreien etc.	1.	
§. 3.	Lehrsatz. Die Anzahl dieser Producte ist $=2^\nu$.	5.	§. 2.
§. 4.	Lehrsatz. Der Werth eines Products ändert sich nicht durch beliebige *Weglassung* der Multiplicationszeichen.	6.	§. 1 u. 3.
§. 5.	Lehrsatz. ν Elemente können auf nicht mehr als $1.2.3 \ldots \nu$ Arten in verschiedener Ordnung mit einander verbunden werden.	13.	§. 4.
§. 6.	Lehrsatz. Die Ordnung der Aufeinanderfolge der Factoren eines Products kann nach Belieben verändert werden, ohne daſs sich der Werth des Products änderte.	16.	§. 2, 4 u. 5.
§. 7.	Lehrsatz. Die Vorzeichen + und — der Factoren eines und desselben Products von ν Factoren lassen sich auf $2^{\nu-1}$ Arten verändern.	23.	
§. 8.	Erklärungen. Reste, Summen und Quotienten betreffend.	24.	
§. 9.	Erläuterungen zu §. 8.	27.	§. 8.
§. 10.	Erklärungen und Erläuterungen. Congruenzen und das Zeichen 𝔖 betreffend.	29.	§. 9.
§. 11.	Lehrsatz. Sätze das Zeichen 𝔖 betreffend.	33.	§. 10.
§. 12.	Erklärungen und Erläuterungen. Stammzahlen und theilbare Zahlen betreffend.	39.	§. 10.
§. 13.	Erläuterung. Ganze Zahlen und Brüche betreffend. . .	43.	

	Seite	Nimmt Bezug auf
§. 14. und 15. **Lehrsätze.** Factoren betreffend.	46.	§. 13 u. 14.
§. 16. **Lehrsatz.** Der Quotient ist der nemliche, in welcher Ordnung auch eine Zahl z durch die Factoren einer andern u dividirt werden mag.	48.	§. 13 u. 15.
§. 17. **Lehrsatz.** Der Satz §. 16. gilt unter gewissen Bedingungen auch wenn u in z *nicht* aufgeht.	50.	§. 8, 9, 15 u. 16.
§. 18. **Lehrsatz.** Wenn $z_1 + z_2 + z_3 \ldots\ldots + z_{n-1} + z_n = 0$ ist und u geht in $z_1, z_2, z_3, \ldots\ldots z_{n-1}$ auf, so geht es auch in z_n auf.	58.	§. 14.
§. 19. **Lehrsatz.** Von der Theilergemeinschaft zweier Zahlen. .	58.	§. 8 u. 9.
§. 20. **Lehrsatz.** Wenn u zu z_1 und zu z_2 theilerfremd ist, so ist es auch zu dem *Product* $z_1 z_2$ theilerfremd etc.	64.	§. 18 u. 19.
§. 21. **Erläuterung.** Jede theilbare Zahl kann durch $a^\alpha b^\beta c^\gamma \ldots\ldots n^\nu$ ausgedrückt werden.	66.	
§. 22. **Lehrsatz.** Von der Theilerverwandtheit und Theilerfremdheit zweier Zahlen, nach (§. 21.) ausgedrückt.	67.	§. 20.
§. 23. **Lehrsatz.** Der gröfste Gemeintheiler zweier Zahlen ist das Product aller derjenigen Stammfactoren, welche sie gemein haben.	68.	§. 22.
§. 24. **Lehrsatz.** Wenn u in z aufgeht, so müssen unter den Stammfactoren von z alle die von u sein.	69.	§. 15 u. 20.
§. 25. **Lehrsatz.** Wenn u in $z_1 z_2$ aufgeht und zu z_1 theilerfremd ist, so mufs es in z_2 aufgehen etc.	70.	§. 24.
§. 26. **Lehrsatz.** Wenn z mit $v_1, v_2, v_3, \ldots\ldots v_n$ aufgeht, so geht es auch mit $u = v_1 v_2 v_3 \ldots\ldots v_n$ auf, insofern die v unter einander theilerfremd sind.	71.	§. 13 u. 24.
§. 27. **Lehrsatz.** Eine ganze Zahl kann nur auf eine einzige Art durch die Multiplication von Stammfactoren zusammengesetzt werden.	72.	§. 24.
§. 28. **Lehrsatz.** Von den allgemeinen Ausdrücken der *geraden* und *ungeraden* Zahlen.	72.	
§. 29. **Lehrsatz.** Von der Anzahl, der Summe etc. der Theiler einer Zahl. , .	76.	§. 14, 21, 24 u. 28.
§. 30. **Lehrsatz.** Von den *Zahlensystemen.*	81.	§. 18.
§. 31. **Lehrsatz.** Jede Zahl ist die Summe dieser oder jener Potenzen der Zahl 2, so wie der Zahl 3, letzteres nach Abzug der Summe dieser oder jener Potenzen von 3.	84.	§. 30.

	Seite	Nimmt Bezug auf
§. 32. Lehrsatz. Von den Zahlen, von deren Theilbarkeit diejenige *gröfserer* Zahlen abhängt.	85.	§. 11, 18, 25 u. 30.
§. 33. Aufgabe. Zahlen z, kleiner als gegebene Zahlen Z, zu finden, von deren Theilbarkeit mit der Zahl s die von Z mit s abhängt.	86.	§. 11, 26, 30 u. 32.
§. 34. Lehrsatz. Von der Gleichung $mv = nu + r$.	96.	§. 15, 18 u. 25.
§. 35. Lehrsatz. Von der Gleichung $mv = \mathfrak{G}u + r$ für m nicht $> \frac{1}{2}u$.	104.	§. 25.
§. 36. Lehrsatz. Von den Resten der Zahlen $1, 2, 3, 4, \ldots \frac{1}{2}(uv-1)$ dividirt durch u und v.	106.	§. 18, 26 u. 34.
§. 37. Lehrsatz. Von der Summe der Quotienten μ und ν und der Reste r und ϱ in $(1, 2, 3, 4, \ldots n)m = \mu n + r$ und $(1, 2, 3, 4, \ldots m)n = \nu m + \varrho$.	115.	§. 34.
§. 38. Lehrsatz. Von der Summe der Quotienten μ und ν und den Resten r und ϱ in $(1, 2, 3, 4, \ldots \frac{1}{2}n$ oder $\frac{1}{2}(n-1))m = \mu n + r$ und $(1, 2, 3, 4, \ldots \frac{1}{2}m$ oder $\frac{1}{2}(m-1))n = \nu m + \varrho$.	120.	§. 37.
§. 39. Lehrsatz. Die Anzahl $\varkappa$ derjenigen Reste r in $v = \mu u + r$ für $\mu = 1, 2, 3, 4, \ldots \frac{1}{2}(u-1)$ und ein ungerades $u = 4n \pm 1$, welche $> \frac{1}{2}u$ sind, ist *gerade* oder *ungerade*, je nachdem es die Summe $S\mu$ der Quotienten $+n(v-1)$ ist.	127.	§. 18.
§. 40. Lehrsatz. Der Fermatsche Satz, dafs für jede *Stammzahl* p und für jede Zahl z, die nicht mit p aufgeht, $z^{p-1} = \mathfrak{G}p + 1$ ist. Die Verallgemeinerung folgt (§. 87. und 98.). Ein zweiter Beweis des Satzes steht (§. 88.).	132.	§. 22, 25 u. 34.
§. 41. Lehrsatz. Es ist $z^{\frac{1}{2}(p-1)} = \mathfrak{G}p \pm 1$ für jedes nicht mit p aufgehende z, je nachdem die Anzahl $\varkappa$ der Reste r in $\varepsilon z = \mathfrak{G}p + r$ für $\varepsilon = 1, 2, 3, 4, \ldots \frac{1}{2}(p-1)$, die $> \frac{1}{2}p$ sind, *gerade* oder *ungerade* ist.	134.	§. 25 u. 35.
§. 42. Lehrsatz. Das *Reciprocitäts-* oder *Gegenseitigkeitsgesetz* für Stammzahlen.	136.	§. 28, 36, 38, 39 u. 41.
§. 43. Erklärung. Die Wurzeln von Gleichungen zwischen ganzen Zahlen beliebiger Ordnung betreffend.	142.	
§. 44. Lehrsatz. Die Gleichung $\varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_1 x + \varepsilon_0 = \mathfrak{G}p$ kann, wenn p eine *Stammzahl* ist und die ε *ganze* Zahlen sind, für *nicht mehr* als n positive und ebensoviele negative ganzzahlige Werthe von $x > 0$ und $< p$ Statt finden.	142.	§. 2, 11, 25 34 u. 40.

	Seite	Nimmt Bezug auf
§. 45. Lehrsatz. Erläuterndes von ***Quadratresten*** und ***Nichtquadratresten***. (Die Erweiterung der Benennungen folgt §. 89.) . . .	154.	
§. 46. Erklärung. ***Zusammengehörige*** Zahlen, nemlich Factorenpaare für den Rest r zum Theiler a betreffend. (Die Erweiterung der Benennung folgt §. 89.)	158.	
§. 47. Lehrsatz. Von den ***zusammengehörigen Zahlen***. . . .	159.	**§. 34, 45 u. 46.**
§. 48. Lehrsatz. Der Wilsonsche Satz, dafs für jede ungerade Stammzahl p, $1.2.3.4\ldots(p-1) = \mathfrak{G}p-1$ ist.	161.	**§. 47.**
Zweiter, dritter und vierter Beweis dieses Satzes in §. 73. Fünfter Beweis dieses Satzes §. 93. Die Verallgemeinerung des Satzes für eine ***beliebige*** Zahl z folgt in §. 97.		
§. 49. Lehrsatz. Das Gegenseitigkeitsgesetz in Beziehung auf Quadratreste r und Nichtquadratreste ϱ, und dafs für erstere $r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, für letztere $\varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ für jede ungerade Stammzahl p ist.	162.	**§. 11, 40, 42, 44, 45, 47 u. 48.**
§. 50. Lehrsatz. Auf welche Weise die absoluten Werthe der positiven und negativen echten Quadratreste und Nichtquadratreste ***dieselben*** sind.	167.	**§. 49.**
§. 51. Lehrsatz. Von der ***Summe*** der absoluten Werthe je zweier Quadratreste und Nichtquadratreste.	169.	**§. 49 u. 50.**
§. 52. Lehrsatz. Von den ***Producten*** von Quadratresten und Nichtquadratresten.	171.	**§. 49.**
§. 53. Lehrsatz. Von der Form der Stammzahlen, für welche $+1$, -1, $+2$ und -2 Quadratreste oder Nichtquadratreste sind.	172.	**§. 41, 49 u. 52.**
§. 54. Lehrsatz. Von der Anzahl der Werthe von z, r und ϱ in $z^{\delta} = \mathfrak{G}p+r$ und $z^{\lambda} = \mathfrak{G}p+\varrho$, wenn p eine Stammzahl ist und δ in $p-1$, λ in δ aufgeht.	176.	**§. 11, 40, 43 u. 44.**
§. 55. Lehrsatz. Erweiterung von §. 54.	182.	**§. 12, 19, 40 u. 54.**
§. 56. Lehrsatz. In $z^{\varepsilon} = \mathfrak{G}p+1$, wo p eine Stammzahl ist, kann auch $\varepsilon < p-1$ sein, wenn es nur mit $p-1$ Theiler >1 gemein hat etc. .	188.	**§. 12, 40, 54 u. 55.**
§. 57. Erklärung der Benennungen ***Stammwurzel*** und ***Hauptstammwurzel***, gewöhnlich ***primitive Wurzeln genannt***; so wie der Benennung ***Index***.	191.	**§. 56.**

	Seite	Nimmt Bezug auf
§. 58. **Lehrsatz.** Es giebt für jeden Exponenten δ, der in $p-1$ *aufgeht*, δte Stammwurzeln z_δ aus 1 zu der ***Stammzahl*** p, aber keine für Exponenten, die in δ *nicht* aufgehen.	192.	§. 40 u. 56.
§. 59. **Lehrsatz.** Die Reste der Potenzen von Stammwurzeln aus 1 zu Stammzahlen bilden *Perioden*.	193.	
§. 60. **Lehrsatz.** Die Reste $r_\varkappa$ in $z_\delta^\varkappa = \mathfrak{S}p + r_\varkappa$, für welche λ der *gröſste Gemeintheiler* von $\varkappa$ und δ ist, sind *alle* $\frac{\delta}{\lambda}$ten Stammwurzeln aus 1 zur Stammzahl p etc.	196.	§. 59.
§. 61. **Lehrsatz.** Die Potenzen der *verschiedenen* δten Stammwurzeln aus 1 zu der Stammzahl p lassen zu p *dieselben* Reste, obwohl in verschiedener Ordnung etc.	198.	§. 34 u. 60.
§. 62. **Lehrsatz.** Wenn z_δ in $x^\delta = \mathfrak{S}p + r$ und $(xz_\delta^\varkappa)^\delta = \mathfrak{S}p + \varrho$ eine δte Stammwurzel aus 1 zur Stammzahl p, $\varkappa > 0$ und $< \delta$, x aber eine *beliebige* Zahl ist, so ist $r = \varrho$.	200.	§. 54.
§. 63. **Lehrsatz.** Von der *Anzahl* der Stammwurzeln von gleichen Exponenten; und daſs eine einzige Hauptstammwurzel unmittelbar *alle* Stamm- und Hauptstammwurzeln giebt.	202.	§. 58 u. 60.
§. 64. **Lehrsatz.** Wie die Stammwurzeln aus 1 zur Stammzahl p durch *Ausschlieſsung* zu finden sind.	207.	§. 40, 54 u. 55.
§. 65. **Lehrsatz.** Von den zu einer beliebigen Zahl z theilerfremden Zahlen und von den theilerfremden *Factoren* von z. . .	213.	§. 18. u. 26.
§. 66. **Lehrsatz.** Zehn verschiedene Sätze von Stammwurzeln. .	215.	§. 40, 45, 49, 52, 54, 63 u. 65.
§. 67. **Lehrsatz.** Vier verschiedene Sätze von Stammwurzeln. .	230.	§. 47, 60, 65 u. 66.
§. 68. **Lehrsatz.** Ausdruck der 3ten und 6ten Stammwurzeln aus 1 zu einer Stammzahl $p = 6n + 1$, und Form der Stammzahlen, zu welchen $+3$ und -3 Quadratrest oder Nichtquadratrest sind.	234.	§. 26, 49, 50, 54, 58, 63 u. 66.
§. 69. **Lehrsatz.** Ausdruck der 5ten und 10ten Stammwurzeln aus 1 zu einer Stammzahl $p = 10n + 1$.	241.	§. 54, 63 u. 66.
§. 70. **Aufgabe.** Die Reste der verschiedenen Potenzen einer beliebigen Zahl z, dividirt durch eine andere Zahl $a > z$, bloſs durch Addition und Subtraction zu finden.	246.	§. 40 u. 61.
§. 71. **Aufgabe.** Die Reste einer beliebigen *gleichen* Potenz der Zahlen 1, 2, 3, 4, ..., dividirt durch eine beliebige Zahl a, zu finden. .	249.	§. 31 u. 55.

		Seite	Nimmt Bezug auf
§. 72.	Aufgabe. Die sämmtlichen Stammwurzeln, also auch die Hauptstammwurzeln, zu einer gegebenen Stammzahl p zu berechnen.	252.	§. 45, 63, 64, 66, 70 u. 71.
§. 73.	Drei andere Beweise des Wilsonschen Satzes §. 48.	256.	§. 45, 47, 48, 49, 52, 59 u. 67.
§. 74.	Lehrsatz. Wenn in $a_1\overset{1}{x}+a_2\overset{2}{x}+a_3\overset{3}{x}\ldots+a_n\overset{n}{x}=z$ die x der Reihe nach $m_1, m_2, m_3, \ldots m_n$ verschiedene Werthe bekommen können, während die a dieselben bleiben, so kann z $m_1 m_2 m_3 \ldots m_n$ verschiedene Werthe bekommen; nicht mehr, wohl aber weniger.	258.	
§. 75.	Lehrsatz. Von den Resten r in $E_1x_1+E_2x_2\ldots+E_nx_n = \mathfrak{S}E+r$, wo $E=e_1e_2e_3\ldots e_n$ und $E_1=\frac{E}{e_1}$, $E_2=\frac{E}{e_2}$, ... $E_n=\frac{E}{e_n}$ ist.	261.	§. 18, 27 u. 74.
§. 76.	Lehrsatz. Aus n Reihen von $m_1, m_2, m_3, \ldots m_n$ verschiedenen Gröſsen können $m_1 m_2 m_3 \ldots m_n$ verschiedene Gruppen jede von n Gröſsen zusammengesetzt werden.	265.	
§. 77.	Lehrsatz. Von dem Verhalten der Reste r in $z=m_1e_1+r_1 = m_2e_2+r_2\ldots = m_ne_n+r_n$ zu $E=e_1e_2e_3\ldots e_n$.	266.	§. 26 u. 76.
§. 78.	Lehrsatz. Wenn man z. B. durch φe_1 die Anzahl der Zahlen >0 und $<e_1$ bezeichnet, die zu e_1 *theilerfremd* sind, so ist $\varphi e_1.\varphi e_2.\varphi e_3\ldots\varphi e_n=\varphi(e_1e_2e_3\ldots e_n)$.	269.	§. 14, 65, 74, 75, 76 u. 77.
§. 79.	Lehrsatz. Für $z=xy$, wo x und y beliebig sind, ist $\overset{1}{\varphi}z=x\varphi y$ (78.), wo $\overset{1}{\varphi}z$ die Anzahl der Zahlen >0 und $<z$ bezeichnet, die mit keinem Theiler von y aufgehen.	271.	§. 18 u. 78.
§. 80.	Lehrsatz. Für $z=xy$, wo x und y zu einander *theilerfremd* sind, ist $\overset{2}{\varphi}z=(x-1)\varphi y$ (78.), wo $\overset{2}{\varphi}z$ die Anzahl der Zahlen >0 und $<z$ bezeichnet, die mit keinem Theiler von y und zugleich mit x nicht aufgehen.	276.	§. 18 u. 79.
§. 81.	Lehrsatz. Von den zu einer beliebigen Zahl Z theilerfremden Zahlen Z_φ, ihrer Anzahl φZ, ihrer Summe $S\varphi Z$ und der Theilbarkeit von φZ durch 2.	279.	§. 18, 21, 65, 74, 75, 76, 77, 78 u. 80.
§. 82.	Lehrsatz. Von dem allgemeinen Ausdruck der Glieder des Products $(a_0+a_1+a_2\ldots+a_\alpha)(b_0+b_1+b_2\ldots+b_\beta)\ldots(n_0+n_1+n_2\ldots+n_\nu)$ und ihrer Anzahl.	285.	

	Seite	Nimmt Bezug auf
§. 83. **Lehrsatz.** Wenn man in $z = e\varepsilon$ dem e und dem ε alle ganzzahligen Werthe giebt, die sie haben können, so drückt $\varepsilon . e_\varphi$ (§. 78.) *alle* die Zahlen 1, 2, 3, 4, ... z aus, und jede nur einmal.	287.	
§. 84. **Lehrsatz.** Die Gesammt-Anzahl der zu *allen* Theilern einer beliebigen Zahl z theilerfremden Zahlen, > 0 und kleiner als die einzelnen Theiler, ist $= z$.	290.	§. 63, 74, 75, 76, 77, 78, 81, 82 u. 83.
§. 85. **Lehrsatz.** Wenn in der Gleichung $uv = \mathfrak{S}z + w$ zwei von den drei ganzen Zahlen u, v und w zu z theilerfremd sind, so ist es auch die dritte; und wenn die eine alle z_φ (§. 78.) durchläuft, während eine zweite denselben Werth behält, so durchläuft auch die dritte alle z_φ.	295.	§. 18.
§. 86. **Lehrsatz.** Wenn in $a^\alpha b^\beta c^\gamma n^\nu = \mathfrak{S}z + r$, a, b, c, ... n sämmtlich zu z theilerfremd sind, so ist es auch r.	299.	§. 18.
§. 87. **Lehrsatz.** Der verallgemeinerte Fermatsche Satz (§. 40.). Eine Vereinfachung oder nähere Bestimmung dieses Satzes giebt (§. 98.).	300.	§. 18, 40 u. 85.
§. 88. Zweiter Beweis des Fermatschen Lehrsatzes (§. 40.). . . .	302.	§. 85 u. 87.
§. 89. **Erklärung.** Erweiterung der Benennungen zusammengehörige Zahlen, Quadratreste etc. (§. 45. und 46.).	302.	§. 45 u. 46.
§. 90. **Lehrsatz.** Von den Quadratresten, Quadraten und Quadratwurzeln zu beliebigen Zahlen.	303.	§. 18, 85 u. 89.
§. 91. **Lehrsatz.** Von der *Anzahl* der Werthenpaare von x in $x^2 = \mathfrak{S}z + w$ für eine beliebige Zahl z.	308.	
§. 92. **Lehrsatz.** Wenn z_1, z_2, z_3, ... $z_{\varphi z}$ die sämmtlichen zu z *theilerfremden* Zahlen > 0 und $< z$ sind und n ist die *Anzahl* der Werthenpaare von x in $x^2 = \mathfrak{S}z + 1$, so ist das *Product* $Z = z_1 z_2 z_3 z_{\varphi z} = \mathfrak{S}z \pm 1$, je nachdem n *gerade* oder *ungerade* ist; desgleichen ist $Z = \mathfrak{S}z + w^{\frac{1}{2}\varphi z}$, wenn w ein *Nichtquadratrest* zu z ist. .	309.	§. 85, 90 u. 91.
§. 93. Fünfter Beweis des Wilsonschen Lehrsatzes (§. 48.). . . .	312.	§. 91 u. 92.
§. 94. **Lehrsatz.** Von den Werthen von x in $x^2 = \mathfrak{S}z + r$ für ein beliebiges z, und von der *Anzahl* der x für das nemliche r. .	313.	§. 18, 34, 85, 90, 91 u. 92.
§. 95. **Lehrsatz.** Von der Anzahl der entweder theilerfremden, oder durch keine gröſsere Zahl als 2 gemeintheilbaren Factorenpaare, in welche sich eine beliebige Zahl z zerlegen läſst.	337.	§. 2 u. 3.

	Seite	Nimmt Bezug auf
§. 96. Lehrsatz. Ausdrücke der Anzahl der x und r in $x^2 = \mathfrak{G}z + r$ für ein beliebiges z durch die Anzahl der Factorenpaare von z von der Art (§. 95.).	342.	§. 45, 81, 94 u. 95.
§. 97. Lehrsatz. Für alle *Quadratreste* r zu $z = p^e$, wo p eine Stammzahl $\gt 2$ bezeichnet, ist $r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$ und für alle Nichtquadratreste w ist $w^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$. Desgleichen giebt es zu jeder beliebigen Zahl z, von welcher p ein Stammfactor ist, immer Nichtquadratreste W, die zugleich Nichtquadratreste zu p sind.	344.	§. 34, 40, 45, 49, 81, 89 u. 96.
§. 98. Lehrsatz. Für jede zu $z = 2^m$ theilerfremde Zahl z_φ ist $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$, mit der einzigen Ausnahme der Zahl $z_\varphi = 3$ für $z = 2^2 = 4$.	357.	§. 10, 81 u. 90.
§. 99. Lehrsatz. Verallgemeinerung des Wilsonschen Lehrsatzes (§. 48.).	360.	§. 26, 48, 92, 95, 96, 97 u. 98.
§. 100. Lehrsatz. Vereinfachung oder nähere Bestimmung des verallgemeinerten Fermatschen Lehrsatzes (§. 87.).	365.	§. 57, 81, 87, 94 u. 96.
Tafel I. Sie giebt die Reste r an, welche bleiben, wenn man die 1te, 2te, 3te, ... bis $p - 1 = 60$te Potenz der Zahlen $z = 1, 2, 3, 4, \ldots 60 \; (= p - 1)$ durch die Stammzahl $p = 61$ dividirt.	369.	
Tafel II. Selbige giebt die Reste r an, welche die verschiedenen Potenzen z^λ der Zahlen $z = 1, 2, 3, 4, \ldots p - 1$ lassen, wenn man diese Potenzen durch die Stammzahlen p von $p = 3$ bis $p = 101$ dividirt, also die r in $z^\lambda = \mathfrak{G}p + r$, nebst den zugehörigen z; desgleichen die Hauptstammwurzeln z_{p-1} und die Stammwurzeln z_δ aus 1 zu p für jeden Theiler δ von $p - 1$. Von $p = 3$ bis $p = 29$ giebt sie die r und die z für $\lambda = 2, 3, 4, 5, \ldots p - 2$ an, von $p = 31$ bis $p = 101$ aber nur für diejenigen λ, welche in $p - 1$ aufgehende Stammzahlen sind.	371.	
Tafel III. Selbige giebt die Zahlen an, zu welchen 1, 2, 3, ... 101 Hauptstammwurzeln sind.	387.	

§. 1.

Erklärung und Erläuterung.

Das Zeichen $\times$, oder auch ein ***Punct,*** zwischen die Buchstaben gesetzt, welche Zahlengröfsen bezeichnen, soll anzeigen, dafs das Ergebnifs alles Dessen, was dem Zeichen vorhergeht, mit dem Ergebnifs alles Dessen, was ihm bis ***zum nächsten Zeichen*** folgt, zu ***multipliciren*** sei. Das ***Ergebnifs*** von Multiplicationen dagegen soll durch blofses ***Aneinanderreihen*** der Buchstaben, ohne dazwischen stehende Zeichen, ausgedrückt werden.

Also soll z. B. $a.b.c.d.e$ oder $a\times b\times c\times d\times e$ bezeichnen, dafs zunächst die Zahl a mit der Zahl b, die daraus hervorgehende Zahl mit der Zahl c, die hieraus hervorgehende Zahl mit der Zahl d u. s. w. zu multipliciren sei. Dagegen soll $abcde$ die Zahl bezeichnen, welche das letzte Ergebnifs dieser Multiplicationen ist.

Da auf solche Weise ab das Ergebnifs der durch $a.b$, $a.b.c$ das Ergebnifs der durch $a.b.c$ ***angedeuteten*** Multiplicationen ist u. s. w., so folgt ***aus der blofsen Bedeutung der Zeichen,*** dafs z. B. die Zahl $abcde$ auf folgende verschiedene Arten geschrieben werden kann:

1. $abcde = abcd.e = abc.d.e = ab.c.d.e = a.b.c.d.e.$

Aber es folgt nicht eben so, ohne weitern Beweis, dafs auch z. B.

$abcde = abc.de = ab.cde = ab.cd.e = a.bcde$ u. s. w.

sei. Die Gründe dieser letzteren Gleichheit liegen ***nicht*** in der blofsen Bedeutung der Zeichen.

§. 2.

Lehrsatz.

Das Product

1. $P_\nu = (1+a)(1+b)(1+c)(1+d)\ldots(1+m)(1+n)$,

in welchem a, b, c, d, ... m, n ***beliebige ungleiche Zahlgröfsen sind, deren Anzahl durch*** ν ***bezeichnet werden mag, ist gleich der Summe der Einheit und aller möglichen ungleichen Producte von*** a, b, c, ... m, n, ***zu einem, zwei, drei, vier bis zu*** ν ***ungleichen Factoren, jeden Factor nur einmal genommen. Keines dieser Producte fehlt, und keines kommt mehr als einmal vor. Als ungleich werden alle diejenigen***

Producte betrachtet, von welchen nicht **sämmtliche** *Factoren die nemlichen sind, in welcher Ordnung sie auch sonst auf einander folgen mögen.*

Beispiel. Für die 5 Zahlengröfsen a, b, c, d und e ist

$$2.\quad (1+a)(1+b)(1+c)(1+d)(1+e)$$
$$= 1$$
$$+a+b+c+d+e$$
$$+ab+ac+bc+ad+bd+cd+ae+be+ce+de$$
$$+abc+abd+acd+bcd+abe+ace+bce+ade+bde+cde$$
$$+abcd+abce+abde+acde+bcde$$
$$+abcde.$$

Die Glieder rechts sind hier, aufser der Einheit, *alle möglichen* Producte von *einem, zwei, drei, vier* und *fünf ungleichen* Factoren. Keins fehlt, und keins, desgleichen auch kein Factor, kommt mehr als einmal vor.

Beweis. *A.* Anstatt zu beweisen, dafs das Product $P_\nu = (1+a)(1+b)(1+c)\dots(1+n)$ (1.) die Summe der Einheit und aller möglichen Producte von $a, b, c, \dots m, n$ zu einem, zwei, drei u. s. w. Factoren sei, werde, umgekehrt, bewiesen, dafs die ebengenannte Summe nichts anderes ist, als jenes Product. Daraus wird unmittelbar die Behauptung des Lehrsatzes folgen; denn wenn bewiesen ist, dafs eine Gröfse B einer Gröfse A gleich sei, so folgt auch, dafs nothwendig A gleich B ist.

B. Man nehme einen Augenblick an, die *rechts* in (2.) stehenden Producte seien wirklich *alle möglichen* aus den 5 Factoren a, b, c, d und e, zu *keinem* (was die 1 giebt), zu *einem, zwei, drei, vier* und *fünfen,* von welcher letzten Art offenbar nur das eine Product $abcde$ möglich ist, und es komme nun eine neue *sechste* Gröfse f hinzu.

Unstreitig befinden sich dann unter allen möglichen Producten der sechs Gröfsen a, b, c, d, e und f auch die der fünf Gröfsen a, b, c, d und e. Es sind unter jenen alle diejenigen, die den Factor f *nicht* enthalten, also gerade alle die, welche rechts in (2.) schon vorhanden sind; denn diese Producte sind nach der Voraussetzung *alle möglichen* aus den 5 Gröfsen a, b, c, d und e, *ohne* Rücksicht auf die sechste Gröfse f.

Um daher *alle möglichen* Producte aus den 6 Gröfsen a, b, c, d, e und f zu finden, kommt es nur darauf an, zu allen jenen möglichen Producten aus den 5 Gröfsen a, b, c, d und e noch alle die möglichen Producte hinzuzuthun, welche von der sechsten Gröfse f herrühren; also diejenigen, welche sämmtlich f zum *Factor* haben.

C. Diese ergeben sich wie folgt.

Zu der *zweiten* horizontalen Zeile nemlich rechts in (2.), welche blofs Producte von *einem* Factor enthält, kommt offenbar nur *f* selbst hinzu; denn es giebt kein anderes Product mit dem *einen* Factor *f*. Also ist zu der *zweiten* Zeile noch *f*, multiplicirt mit der 1 aus der *ersten* Zeile, hinzuzuthun.

Was zu der *dritten* horizontalen Zeile rechts in (2.), die nach der Voraussetzung alle möglichen Producte von zwei Factoren aus den 5 Gröfsen *a*, *b*, *c*, *d* und *e* enthält, wegen *f* noch hinzukommt, findet sich, wenn man *alle möglichen* Producte von *einem Factor* aus den 5 Gröfsen *a*, *b*, *c*, *d*, *e* mit *f* multiplicirt; denn dies giebt offenbar *alle die möglichen* Producte von *zwei* Factoren, deren jedes *f* zu einem seiner Factoren hat. Alle möglichen Producte von einem Factor stehen aber in der *zweiten* Zeile, also mufs man diese ganze zweite Zeile mit *f* multipliciren und das Resultat zu der *dritten* hinzuthun. Alsdann enthält die dritte Zeile *alle möglichen* Producte von zwei Factoren aus den 6 Gröfsen *a*, *b*, *c*, *d*, *e* und *f*.

Eben so findet sich, was zu der *vierten* horizontalen Zeile rechts in (2.), die nach der Voraussetzung alle möglichen Producte von *drei* Factoren aus den 5 Gröfsen *a*, *b*, *c*, *d* und *e* enthält, wegen *f* noch hinzukommt, wenn man *alle möglichen* Producte von *zwei* Factoren aus den 5 Gröfsen *a*, *b*, *c*, *d* und *e* mit *f* multiplicirt; denn das giebt offenbar alle die *möglichen* Producte von *drei* Factoren, deren jeder *f* zu einem seiner Factoren hat. Alle die möglichen Producte von 2 Factoren stehen aber in der *dritten* Zeile: also mufs man diese ganze dritte Zeile mit *f* multipliciren und das Resultat zu der *vierten* hinzuthun. Alsdann enthält diese vierte Zeile *alle möglichen* Producte von drei Factoren aus den 6 Gröfsen *a*, *b*, *c*, *d*, *e* und *f*.

Gleicherweise verhält es sich mit den folgenden Zeilen. Man mufs die ganze *vierte* Zeile mit *f* multipliciren und das Resultat zur *fünften* hinzuthun, worauf diese alle möglichen Producte von vier Factoren aus den 6 Gröfsen *a*, *b*, *c*, *d*, *e* und *f* enthält. Und so weiter.

Zuletzt kommt durch das eine mögliche Product *abcdef aller* 6 Gröfsen *a*, *b*, *c*, *d*, *e* und *f* eine neue 7te Zeile hinzu, die aber gleichmäfsig entsteht, wenn man die 6te Zeile, die nur das eine, aus den 5 Gröfsen *a*, *b*, *c*, *d* und *e* mögliche Product von 5 Factoren enthält, noch mit *f* multiplicirt.

D. Um daher *alle möglichen* Producte, von keinem, einem, zwei, drei u. s. w. Factoren aus *sechs* Gröfsen aus der Gesammtheit aller möglichen Producte von keinem, einem, zwei, drei u. s w. Factoren aus *fünf* Gröfsen zu

finden, ist nichts weiter nöthig, als *jede* Zeile der letzteren, folglich die ***Gesammtheit*** derselben, mit der neuen sechsten Gröfse f zu multipliciren und das Resultat zu der Gesammtheit der Producte aus 5 Gröfsen hinzuzuthun.

E. Ob nun aber gerade 5 Gröfsen, wie in dem Beispiel, zuerst vorhanden sind, und eine neue sechste hinzukommt, oder ob anfangs weniger oder mehr Gröfsen vorhanden sind, ändert offenbar an dem Obigen nichts. Welche Zahl von Gröfsen auch zuerst vorhanden sein mag: immer ist, um aus der Gesammtheit der Producte von keinem, einem, zwei, drei u. s. w. Factoren aus ihrer Mitte die Gesammtheit der Producte für ***eine Gröfse mehr*** zu finden, nichts weiter nöthig, als die schon vorhandenen Producte sämmtlich noch mit der ***neuen*** Gröfse zu multipliciren und das Resultat zu den vorhandenen Producten hinzuzuthun.

F. Wären also ursprünglich statt der 5 Gröfsen a, b, c, d, e allgemein die $\nu-1$ Gröfsen $a, b, c, d, \ldots m$ vorhanden, bezeichnete man die Gesammtheit ***aller möglichen*** Summen ihrer Producte von keinem, einem, zwei, drei u. s. w. Factoren durch $S_{\nu-1}$, und käme nun eine neue, νte Gröfse n hinzu, so würde die Gesammtheit oder die Summe ***aller möglichen*** Producte von keinem, einem, zwei, drei etc. Factoren aus den ν Gröfsen $a, b, c, d, \ldots n$, welche S_ν ausdrückt, gefunden werden, wenn man $S_{\nu-1}$ mit n multiplicirt und das Resultat noch zu $S_{\nu-1}$ hinzuthut. Also würde

$$3. \quad S_\nu = S_{\nu-1} + n \,.\, S_{\nu-1} = (n+1) S_{\nu-1}$$

sein.

G. Was aber für ν gilt, gilt auch zufolge (***E.***) für $\nu-1$, oder für den Fall, wenn ursprünglich nur die $\nu-2$ Gröfsen $a, b, c, d, \ldots l$ vorhanden wären und die $\nu-1$te neue Gröfse m hinzukäme. Also ist vermöge (3.) auch

$$4. \quad S_{\nu-1} = (m+1) S_{\nu-2},$$

und dies, in (3.) gesetzt, giebt

$$5. \quad S_\nu = (m+1)(n+1) S_{\nu-2}.$$

Eben so gilt, was für $\nu-1$ gilt, auch für $\nu-2$, oder für den Fall, wenn ursprünglich nur $\nu-3$ Gröfsen $a, b, c, d, \ldots k$ vorhanden wären und es käme die $\nu-2$te neue Gröfse l hinzu. Also ist vermöge (3.) auch

$$6. \quad S_{\nu-2} = (l+1) S_{\nu-3},$$

und dies, in (5.) gesetzt, giebt

$$7. \quad S_\nu = (l+1)(m+1)(n+1) S_{\nu-3}.$$

H. So findet sich weiter

$$8.\quad \begin{cases} S_\nu = (k+1)(l+1)(m+1)(n+1)S_{\nu-4}, \\ S_\nu = (i+1)(k+1)(l+1)(m+1)(n+1)S_{\nu-5}, \\ \ldots\ldots\ldots\ldots \end{cases}$$

und zuletzt

$$9.\quad S_\nu = (n+1)(m+1)(l+1)(k+1)\ldots(b+1)S_1.$$

I. Aber die Gesammtheit oder die Summe S_1 der Producte für *blofs eine* Gröfse a, welche S_1 bezeichnet, ist offenbar $1+a$; denn aufser der Einheit giebt es aus blofs einer Gröfse a kein anderes Product als a selbst. Also ist schliefslich

$$10.\quad S_\nu = (1+a)(1+b)(1+c)(1+d)\ldots(1+m)(1+n).$$

K. Es findet sich also, dafs die Gesammtheit oder die Summe S_ν *aller möglichen* Producte von keinem, einem, zwei, drei etc. Factoren aus den ν Gröfsen $a, b, c, d, \ldots n$, so genommen, dafs keines mehr als einmal vorhanden ist, und keines fehlt, auch keine Gröfse mehr denn einmal als Factor vorkommt, durch das *Product* P_ν (1.) der ν Gröfsen $1+a, 1+b, 1+c, \ldots \ldots 1+n$ ausgedrückt wird. Mithin ist auch umgekehrt das Product P_ν *dieser* Gröfsen gleich der Gesammtheit S_ν aller möglichen Producte von keinem, einem, zweien, dreien etc. aus den ν Gröfsen $a, b, c, d, \ldots n$.

L. Anm. Das Hauptmoment des Beweises ist, dafs aus der Gesammtheit aller möglichen Producte von keinem, einem, zwei, drei etc. Factoren einer beliebigen Zahl von Gröfsen $a, b, c, d, \ldots$ die Gesammtheit der Producte für *eine Gröfse mehr* gefunden wird, wenn man jene Gesammtheit mit der neuen Gröfse multiplicirt und das Resultat zu jener Gesammtheit hinzuthut.

§. 3.

Lehrsatz.

Die Anzahl aller möglichen Producte von einer, zwei, drei etc. bis zu ν aus ν beliebigen Gröfsen oder Zahlen a, b, c, d, ... m, n *ist, wenn man noch die Einheit, diese gleichsam als Product keines jener Factoren, hinzuthut, gleich* 2^ν.

Beispiel. Für 5 Zahlen a, b, c, d und e sind folgende Producte möglich.

1.
Das 1 Product mit keinem Factor, 1.
Die 5 Producte von 1 Factor, nemlich *a, b, c, d, e.*
Die 10 Producte von 2 Factoren, nemlich *ab, ac, ad, ae, bc, bd be, cd, ce, de.*
Die 10 Producte von 3 Factoren, nemlich *abc, abd, abe, acd, ace, ade, bcd, bce, bde, cde.*
Die 5 Producte von 4 Factoren, nemlich *abcd, abce, abde, acde, bcde.*
Das 1 Product von 5 Factoren, nemlich *abcde.*

Thut zusammen 32 Producte, und für $\nu = 5$, wie hier, ist $2^\nu = 2^5 = 32$.

Beweis. Zufolge (§. 2.) enthält das Product

$$2.\quad P_\nu = (1+a)(1+b)(1+c)(1+d)\ldots(1+n),$$

wenn man es entwickelt, nächst der Einheit, *alle möglichen* Producte aus den ν Factoren $a, b, c, d, \ldots n$ zu einem, zwei, drei etc. bis ν; und keines dieser Producte mehr als einmal.

Für beliebig *bestimmte* Zahlenwerthe von $a, b, c, d, \ldots n$ findet man den *Zahlenwerth* des Products P_ν offenbar eben sowohl, wenn man den Buchstaben $a, b, c, d, \ldots n$ in (2.), als wenn man ihnen in den *einzelnen Gliedern* des *entwickelten* Products die ihnen bestimmten Zahlenwerthe beilegt; und zwar *immer, welche* auch die Zahlenwerthe von $a, b, c, d, \ldots n$ sein mögen.

Macht man nun z. B. $a = b = c = d \ldots = n = 1$, so ist der Zahlenwerth *jedes* Gliedes des *entwickelten* Products *gleich 1*, und folglich die *Summe* dieser Glieder, das heifst P_ν, ihrer *Anzahl* gleich. Andrerseits ist für $a = b = c = d \ldots = n = 1$, zufolge (2.), $P_\nu = (1+1)(1+1)(1+1)\ldots(1+1)$, oder, da P_ν ν Factoren hat, $= 2^\nu$; mithin ist die *Anzahl* der Glieder des entwickelten Products P_ν gleich 2^ν.

§. 4.

Lehrsatz.

Der Werth eines Products beliebiger ganzer Zahlen a, b, c, d, … … m, n, *deren Anzahl durch* ν *bezeichnet werden mag, bleibt derselbe, man mag erst* a *mit* b, *das Ergebnifs davon mit* c, *das Ergebnifs davon mit* d *u. s. w. multipliciren, oder man mag das Ergebnifs der Multiplication einiger ersten Factoren mit dem Ergebnifs der Multiplication einiger folgenden, u. s. w. bis zu Ende, multipliciren. Es wird indessen*

einstweilen vorausgesetzt, dafs bei der einen und der andern Art der Multiplicationen die Factoren in der gleichen Aufeinanderfolge in Rechnung kommen.

In dem Sinne der Bedeutung des Vorhandenseins oder der Abwesenheit des Puncts als Multiplicationszeichen (§. 1.), dafs nemlich das Vorhandensein des Puncts die Operation und die Abwesenheit desselben das Resultat derselben andeutet, behauptet der Lehrsatz, dafs z. B. in dem Product

$$1.\quad P_\nu = a.b.c.d.e \ldots i.k.l.m.n$$

die Puncte, wo man will, und ihrer so viele, als man will, weggelassen werden können, ohne dafs der Werth des Products sich änderte.

Übrigens können die Zahlengröfsen a, b, c, d, ... n *unter einander sämmtlich ungleich, oder einige davon, oder alle können einander gleich sein. Der Satz bleibt derselbe.*

Beispiel. Es ist

$$2.\quad \begin{cases} 4.6.5.3.9 \\ = 4.6.5.27 = 4.6.15.9 = 4.30.3.9 = 24.5.3.9 \\ = 4.6.135 = 4.90.9 = 120.3.9 = 4.30.27 = 24.5.27 \\ \qquad = 24.15.9 \\ = 4.810 = 24.315 = 120.27 = 360.9 \\ = 3240. \end{cases}$$

In der ersten horizontalen Reihe (2.) ist *kein* Punct weggelassen; in der zweiten Zeile ist je *ein* Punct; in der dritten Zeile sind auf alle mögliche Weise *zwei* Puncte weggelassen; in der vierten Zeile *drei* Puncte, und in der fünften Zeile alle *vier* Puncte.

Beweis. *A.* Man bezeichne der Kürze wegen

$$3.\quad \begin{cases} a.b.c.d \ldots i.k.l.m.n \text{ durch } P, \\ a.b.c.d \ldots i.k.l.m \text{ durch } M, \\ a.b.c.d \ldots i.k.l \text{ durch } L, \\ a.b.c.d \ldots i.k \text{ durch } K, \\ a.b.c.d \ldots i \text{ durch } I, \\ \text{u. s. w.}; \end{cases}$$

so dafs also, der Bedeutung (§. 1.) des Multiplicationspunctes gemäfs,

$$4.\quad \begin{cases} P = M.n = L.m.n = K.l.m.n = I.k.l.m.n, \\ M = L.m = K.l.m = I.k.l.m, \\ L = K.l = I.k.l, \\ K = I.k \end{cases}$$

u. s. w. ist.

B. Nun bedeutet der Ausdruck $L.m.n$ von P in der ersten Zeile (4.), dafs L erst mmal und dann das was herauskommt nmal genommen werden soll. Man schreibe L in einer horizontalen Zeile mmal neben einander, und n solcher Zeilen, nemlich:

$$5.\quad \left.\begin{array}{l} \overbrace{L, L, L, L, \ldots. L}^{m} \\ L, L, L, L, \ldots. L \\ L, L, L, L, \ldots. L \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ L, L, L, L, \ldots. L \end{array}\right\} n,$$

so ist hier L wirklich erst mmal genommen, und dann das Ergebnifs nmal. Also stellt die *Gesammtheit* der L in (5.) P vor.

Aber die *Anzahl* der in (5.) vorhandenen L ist offenbar der *Zahl* mn gleich, denn es sind der L so viele vorhanden als das *Product* mmal n Einheiten hat, also mn. Folglich ist P auch nichts anderes als L, mnmal genommen, und folglich ist auch

$$6.\quad P = L.mn = a.b.c.d \ldots. i.k.l.mn,$$

und daraus folgt, dafs der Werth P sich nicht ändert, wenn man in seinem Ausdruck (1.) den *letzten* Punct wegläfst.

Wir haben also bis jetzt folgende *zwei* verschiedene Ausdrücke von P:

$$7.\quad \begin{cases} P = L.m.n & (4.) \text{ und} \\ P = L.mn & (6.). \end{cases}$$

C. Nun ist in diesen Ausdrücken L nichts anderes als $K.l$ (3.), also kann P vermöge (6.) auch wie folgt geschrieben werden:

$$8.\quad P = K.l.mn.$$

Es zeigte sich aber so eben, dafs, wenn eine Zahl L erst m, und dann das was herauskommt nmal genommen wird, das Ergebnifs das nemliche ist, als wenn man L sogleich mnmal nimmt. Also wird auch in (8.), wo die Zahl K erst mit l und dann das was herauskommt mit *der Zahl* mn multiplicirt werden soll, das Ergebnifs das nemliche sein, als wenn man K sogleich mit dem Product lmn der beiden *Zahlen* l und mn multiplicirt. Mithin ist auch

$$9.\quad P = K.lmn = a.b.c.d \ldots. i.k.lmn \ (3.);$$

und daraus folgt, dafs der Werth von P sich wiederum nicht ändert, wenn man in seinem Ausdruck die *beiden* letzten Puncte wegläfst.

D. Gesetzt nun, es wäre K, statt wie in (8.) erst mit der Zahl l und dann das Ergebnifs mit der Zahl mn, vielmehr K erst mit der *Zahl* lm und dann das Resultat davon mit der *Zahl* n zu multipliciren, so würde das Ergebnifs, aus *gleichem* Grunde wie in (*C.*), $= K.lmn$ sein. Dieses aber ist $= P$ (9.). Also kann P auch durch

$$10. \quad P = K.lm.n = a.b.c.d \ldots i.k.lm.n$$

ausgedrückt werden; und daraus folgt, dafs der Werth von P sich auch nicht verändert, wenn man in seinem Ausdruck (1.) den *vorletzten* Punct wegläfst. Es dürfen also in dem Ausdrucke von P (1.) sowohl die *beiden letzten* Puncte, nach (9.), als der letzte Punct, nach (8.), oder der vorletzte Punct, nach (10.), weggelassen werden, ohne den Werth von P zu ändern.

Demnach haben wir bis hierher folgende *vier* verschiedene Ausdrücke von P:

$$11. \quad \begin{cases} P = K.l.m.n \ (4.), \\ P = K.l.mn \ (8.), \\ P = K.lm.n \ (10.), \\ P = K.lmn \ (9.). \end{cases}$$

E. Man setze in diesen 4 Ausdrücken von P statt K seinen Werth $I.k$ (4.), so erhält man aus (11.) folgende *4 neue Ausdrücke* von P:

$$12. \quad P = I.k.l.m.n = I.k.l.mn = I.k.lm.n = I.k.lmn.$$

In die 2 Ausdrücke von P (7.) dagegen setze man aus (4.) den Werth $I.k.l$ von L, der auch, eben so wie zufolge $L.m.n = Lmn$, nichts anderes ist als $I.kl$, so erhält man noch folgende *2 Ausdrücke* von P:

$$13. \quad P = I.kl.m.n = I.kl.mn.$$

Man setze endlich in den Ausdruck $M.n$ von P (4.) den Werth $I.k.l.m$ von M, der aus demselben Grunde, aus welchem zufolge (*C.*) $K.l.m.n = K.lmn$ war, nichts anderes als $I.klm$ ist, so erhält man noch folgenden *1 Ausdruck* von P:

$$14. \quad P = I.klm.n,$$

und dieser Ausdruck giebt, aus demselben Grunde, aus welchem zufolge (*B.*) $L.m.n = L.mn$ war, endlich noch den *1 Ausdruck*

$$15. \quad P = I.klmn.$$

Zusammen also haben wir nun aus (12. 13. 14. und 15.) $4+2+1+1 = 8$ verschiedene Ausdrücke von P. Sie sind, wenn man sie so ordnet, wie in ihnen *keiner*, oder *einer*, oder *zwei*, oder *drei* Puncte zwischen k, l, m und n *fehlen*, folgende:

$$16.\ \begin{cases} P = I.k.l.m.n\ (12.), \\ P = I.k.l.mn\ (12.) = I.k.lm.n\ (12.) = I.kl.m.n\ (13.), \\ P = I.k.lmn\ (12.) = I.kl.mn\ (13.) = I.klm.n\ (14.), \\ P = I.klmn\ (15.). \end{cases}$$

Keiner dieser Ausdrücke ist seiner *Form* nach dem andern gleich; denn die 4 Ausdrücke (12.) entstanden aus den 4 unter sich verschiedenen Ausdrücken (11.) durch Hinzuthun von *k*, *mit* einem Punct zwischen *k* und *l*; die 2 Ausdrücke (13.) entstanden aus den beiden unter sich verschiedenen Ausdrücken (7.), ebenfalls durch Hinzuthun von *k*, oder *ohne* Punct zwischen *k* und *l*, jedoch mit einem Punct zwischen *l* und *m*, und sind also durch das *Erste* von den vorigen wesentlich verschieden; der eine Ausdruck (14.) entstand aus (4.) durch Hinzuthun von *k*, *l* und *m*, *ohne* Punct zwischen *k* und *l* und *l* und *m*, aber *mit* einem Punct zwischen *m* und *n*, und ist also dadurch ebenfalls von allen vorigen verschieden. Der Ausdruck (15.) hat gar keinen Punct zwischen *k*, *l*, *m* und *n*, während alle vorigen wenigstens einen Punct hatten, und ist also ebenfalls von allen vorigen verschieden.

F. Man setze weiter in die 8 Ausdrücke von *P* (16.) den Werth *H.i* von *I*. (4.), so bekommt man *8 neue Ausdrücke* von *P*, die, eben wie die 8, aus welchen sie entstanden, unter sich verschieden sind, und sämmtlich zwischen *i* und *k* einen Punct haben. Es sind folgende:

$$17.\ \begin{cases} P = H.i.k.l.m.n, \\ P = H.i.k.l.mn = H.i.k.lm.n = H.i.kl.m.n, \\ P = H.i.k.lmn = H.i.kl.mn = H.i.klm.n, \\ P = H.i.klmn. \end{cases}$$

In die 4 Ausdrücke von *P* (11.) setze man den Werth *H.i.k* von *K* (4.), der zufolge (*B*.) nichts anderes ist als *H.ik*, so bekommt man *4 Ausdrücke* von *P*, die, eben wie die 4, aus welchen sie entstanden, *unter sich*, aber auch von den vorigen 8 *dadurch* verschieden sind, dafs sie sämmtlich, anders wie diese, zwischen *i* und *k keinen* Punct haben, wiewohl alle zwischen *k* und *l* einen Punct. Es sind folgende:

$$18.\ \begin{cases} P = H.ik.l.m.n, \\ P = H.ik.l.mn = H.ik.lm.n, \\ P = H.ik.lmn. \end{cases}$$

In die 2 Ausdrücke (7.) von *P* setze man den Werth *H.i.k.l* von *L* (4.), der zufolge (*C*.) nichts anderes ist als *H.ikl*, so bekommt man ferner *2 Ausdrücke* von *P*, die, eben wie die 2, aus welchen sie entstanden,

unter sich, aber auch von allen vorigen ***dadurch*** verschieden sind, dafs sie, anders wie diese, weder zwischen i und k, noch zwischen k und l einen Punct haben, wiewohl beide zwischen l und m einen Punct. Es sind folgende:

$$19.\quad \begin{cases} P = H.ikl.m.n \text{ und} \\ P = H.ikl.mn. \end{cases}$$

In den einen Ausdruck $P = M.n$ (4.) setze man den Werth $H.i.k.l.m$ von M, der zufolge (E.) nichts anderes ist als $H.iklm$, so erhält man

$$20.\quad P = H.iklm.n;$$

welcher Ausdruck wieder von allen vorigen dadurch ***verschieden*** ist, dafs er, anders wie sie, weder zwischen i und k, wie (17.), noch zwischen k und l, wie (18.), noch zwischen l und m, wie (19.), einen Punct hat, sondern nur noch zwischen m und n.

Endlich giebt (20.) vermöge (B.) noch den Ausdruck

$$21.\quad P = H.iklmn,$$

welcher wieder von allen vorigen ***dadurch*** verschieden ist, dafs er nirgend zwischen den Factoren i, k, l, m und n einen Punct hat.

Wir haben also nun zusammengenommen aus (17. 18. 19. 20. und 21.)

$$22.\quad 8+4+2+1+1 = 16$$

Ausdrücke von P, die ***alle*** unter einander ***verschieden*** sind. Sie sind, auf die Weise geordnet, wie zwischen i, k, l, m und n ***keiner***, oder ***einer***, oder ***zwei***, oder ***drei***, oder alle ***vier*** Puncte ***fehlen***, folgende:

$$23.\quad \begin{cases} P = H.i.k.l.m.n \ (17.) \\ P = H.i.k.l.mn \ (17.) = H.i.k.lm.n \ (17.) = H.i.kl.m.n \ (17.) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = H.ik.l.m.n \ (18.), \\ P = H.i.k.lmn \ (17.) \quad = H.i.kl.mn \ (17.) = H.ik.l\,mn \ (18.) \\ \quad = H.i.klm.n \ (17.) = H.ik.lm.n \ (18.) = H.ikl.m.n \ (19.), \\ P = H.i.klmn \ (17.) \quad = H.ik.lmn \ (18.) \quad = H.ikl.mn \ (19.) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = H.iklm.n \ (20.), \\ P = H.iklmn \ (21.). \end{cases}$$

G. Verfährt man von Neuem ganz ähnlich wie in (F.), indem man nemlich in die 16 Ausdrücke von P (23.) statt H seinen Werth $G.h$, in die 8 Ausdrücke (16.) statt I seinen andern Ausdruck $G.hi$, in die 4 Ausdrücke (11.) statt K seinen dritten Ausdruck $G.hik$, in die 2 Ausdrücke (7.) statt L seinen vierten Ausdruck $G.hikl$ und in den 1 Ausdruck (4.) statt M seinen fünften Ausdruck $hiklm$ setzt, so bekommt man, mit $P = G.hiklm.n$ $= G.hiklmn$ zusammengenommen,

$$24. \quad 16+8+4+2+1+1=32$$

Ausdrücke von *P*, die, aus ganz ähnlichen Gründen wie in (*F.*), alle von einander verschieden sind.

H. So also kommen, wenn man auf diese Weise weiter fortfährt, durch jede neue Operation immer gerade *ebensoviele neue*, unter sich und von den vorigen verschiedene Ausdrücke von *P* zum Vorschein, *als zusammengenommen bis dahin vorhanden waren.* Die Zahl der verschiedenen Ausdrücke von *P* wird also durch jede Substitution gerade *verdoppelt.*

Zuerst waren 2 Ausdrücke (7.) von *P* vorhanden. Durch die nächste Substitution stieg ihre Zahl auf das *Doppelte*, auf 4 (11.); durch die folgende Substitution wieder auf das *Doppelte*, auf 8 (16.); sodann abermals auf das *Doppelte*, auf 16 (23.) u. s. w. In den 2 Ausdrücken (7.) enthielt *L* noch $\nu-2$ Factoren; in den $4=2^2$ Ausdrücken (11.) enthielt *K* noch $\nu-3$ Factoren; in den $8=2^3$ Ausdrücken (16.) enthielt *I* noch $\nu-4$ Factoren; in den $16=2^4$ Ausdrücken (23.) enthielt *H* noch $\nu-5$ Factoren. Fährt man also so fort, bis *A* nur noch den *einen* $=(\nu-(\nu-1))$ Factor *a* enthält, das heifst, bis *P*, wie in (1.), *ganz* durch seine einzelnen Factoren ausgedrückt ist, so wird man $2^{\nu-1}$ Ausdrücke von *P* gefunden haben, die in der Form *sämmtlich* unter sich *verschieden* sind; und zwar *dadurch*, dafs ihnen entweder *keiner*, oder, hier oder dort, immer an verschiedenen Stellen, *einer*, oder *zwei*, oder *drei* u. s. w., oder *alle* Puncte fehlen.

I. Fragt man nun gegenseits, auf wievielerlei *Arten* in dem Ausdruck

$$25. \quad P_\nu = a.b.c.d....i.k.l.m.n \ (1.)$$

von den $\nu-1$ Puncten zwischen den ν Factoren *a, b, c, d, ... n* *keiner*, oder *einer*, oder *zwei*, oder *drei* u. s. w. bis $\nu-1$ Puncte fehlen *können*, so ist diese Frage keine andere, als auf wievielerlei Arten sich $\nu-1$ *Dinge* zu 0, 1, 2, 3, ... $\nu-1$ *verbinden* lassen; etwa zu Producten, wenn sie Zahlen wären: denn die *Puncte* sind zwar nicht *an sich selbst* von einander verschieden, aber sie sind es durch ihre *Stellung;* und in Rücksicht auf *diese* können sie allerdings mit $\nu-1$ von einander *verschiedenen* Dingen, z. B. Zahlen oder Factoren, *verglichen* werden. In solchem Betracht ist also die Frage dieselbe, wie die, welches die Zahl der *verschiedenen* möglichen Producte von $\nu-1$ Factoren zu 0, 1, 2, 3, ... $\nu-1$ sei.

Diese Zahl ist zufolge des Lehrsatzes (§. 3.)

$$26. \quad = 2^{\nu-1};$$

also ist auch die Zahl aller möglichen verschiedenen *Arten*, wie in dem Aus-

druck von **P** (25.) 0, 1, 2, 3, ... $\nu - 1$ von den $\nu - 1$ Puncten zwischen den ν Factoren *a, b, c, d, ... n* *weggelassen* werden können, $= 2^{\nu-1}$.

Gerade soviele, durch Weglassung der Puncte *verschiedene* Ausdrücke von **P** wurden aber oben gefunden (*H.*), und es zeigte sich, dafs alle diese verschiedenen Ausdrücke von **P** denselben *Werth* haben. Also wurden *alle möglichen,* der Form nach verschiedenen Ausdrücke von **P** gefunden, und es folgt mithin, dafs der Werth von **P** sich nicht ändere, *welche* und *wieviele* Puncte man auch zwischen den Factoren weglassen möge; was zu beweisen war.

K. Da übrigens der Beweis von den *Werthen* der Factoren *a, b, c, d, ... n* gar nicht abhängt, so folgt auch, dafs es gleichgültig ist, ob die die Factoren unter einander ungleich oder gleich sind.

Anm. Die Hauptmomente des Beweises sind, erstlich, die auf der *Anschauung* beruhende Bemerkung in (*B.*), dafs der *letzte* Multiplicationspunct zwischen den Factoren weggelassen werden könne; sodann die Bemerkung in (*D.*), dafs, da z. B. *k.l.mn,* eben nach der vorigen Bemerkung, dasselbe geben würde, wie *k.lm.n,* nemlich beides *k.lmn,* auch der *vorletzte* Punct *statt* des letzten weggelassen werden könne; und dann endlich der Umstand, dafs die Zahl der sämmtlich unter einander verschiedenen Ausdrücke von **P,** die sich mit Hülfe der beiden vorigen Bemerkungen finden, wie es in (*H.* und *I.*) sich zeigt, gerade *eben so grofs* ist, als, zufolge des Lehrsatzes (§. 3.), die Zahl aller möglichen *Verbindungen* der $\nu - 1$ Multiplicationspuncte zu *keinem, einem, zwei, drei* u. s. w. bis $\nu - 1$.

§. 5.

Lehrsatz.

Es können ν Elemente (z. B. Buchstaben oder Zahlen)

1. a, c, c, d, ... m, n

auf

2. $\overset{\nu}{x} = 1.2.3.4.5 \ldots \nu,$

und nicht mehr und nicht weniger Arten, die der Aufeinanderfolge nach verschieden sind, aneinandergereiht oder mit einander verbunden werden.

Beispiel. Die vier Buchstaben *a, b, c, d* können auf folgende verschiedene Arten nebeneinander gestellt werden:

3.

abcd	*acbd*	*bacd*	*bcad*	*cbad*	*cabd*
abdc	*adbc*	*badc*	*bdac*	*dabc*	*dbac*
adcb	*acdb*	*dacb*	*dcab*	*cadb*	*cdab*
dbca	*dcba*	*bdca*	*bcda*	*cdba*	*cbda.*

ν ist hier 4, und die Zahl der verschiedenen Verbindungen ist, wie man sieht,

$$4.\quad 24 = 1.2.3.4 = 1.2 \ldots \nu.$$

Erster Beweis. *A.* Man lasse irgend *einen* der ν Buchstaben *a, b, c, d, ...* *n*, z. B. *n*, weg, und stelle sich *alle möglichen*, der Aufeinanderfolge nach *verschiedenen* Verbindungen der *übrigen* $\nu-1$ Buchstaben vor. Ihre Anzahl werde durch $\overset{\nu-1}{x}$ bezeichnet. Hängt man nun jeder dieser Verbindungen den einen weggelassenen Buchstaben noch an, so wird man $\overset{\nu-1}{x}$ sämmtlich der Aufeinanderfolge nach unter sich verschiedene Verbindungen haben, und es giebt ihrer nicht mehr und nicht weniger *von denen*, welche alle *n* zum *letzten* Buchstaben haben.

B. Aber statt *n* kann man auch *jeden andern* der ν Buchstaben erst weglassen, alle möglichen, der Aufeinanderfolge nach verschiedenen Verbindungen der *übrigen* machen, und dann diesen Verbindungen jedesmal den zuerst weggelassenen Buchstaben wieder anhängen. Dieses giebt für *jeden* Buchstaben, den man zuerst wegliefs, und dann wieder anhängte, $\overset{\nu-1}{x}$ unter sich verschiedene Verbindungen; nicht mehr und nicht weniger; also überhaupt, da ν Buchstaben vorhanden sind, und *jeder* der *letzte* sein kann, ν *Gruppen*, jede von $\overset{\nu-1}{x}$ Verbindungen; und alle diese Verbindungen sind unter sich verschieden, nicht allein die in jeder Gruppe unter sich, sondern auch die in den verschiedenen Gruppen, weil jede *Gruppe* einen *andern letzten* Buchstaben hat. Desgleichen sind nicht mehr und nicht weniger als ν *Gruppen* möglich, weil jede Gruppe nothwendig *einen* Buchstaben zu ihrem *letzten* hat.

Also sind überhaupt

$$5.\quad \nu.\overset{\nu-1}{x} = \overset{\nu}{x}$$

sämmtlich der Aufeinanderfolge nach verschiedene Verbindungen von ν Buchstaben möglich; nicht mehr und nicht weniger.

C. Was nun von der Zahl ν gilt, gilt auch von jeder andern Zahl der Elemente; also auch von den Zahlen $\nu-1$, $\nu-2$, $\nu-3$, ..., mithin der Reihe nach von den Zahlen 2, 3, 4, ... ν.

Für $\nu=2$, also $\nu-1=1$, ist aber offenbar $\overset{\nu-1}{x} = \overset{1}{x} = 1$; denn *ein* Element läfst sich nur auf $\overset{1}{x} = 1$ Art stellen. Setzt man daher in (5.) der Reihe nach 2, 3, 4, 5, ... ν statt ν, so ergiebt sich

$$6.\quad \begin{cases} 2.1 = \overset{2}{x}, \\ 3.\overset{2}{x} = 3.2 = \overset{3}{x}, \\ 4.\overset{3}{x} = 4.3.2 = \overset{4}{x}, \\ 5.\overset{4}{x} = 5.4.3.2 = \overset{5}{x}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \nu.(\nu-1)(\nu-2)(\nu-3)\ldots.\, 2 = 1.2.3.4.5\ldots.\,\nu = \overset{\nu}{x}; \end{cases}$$

wie es der Lehrsatz behauptet.

Zweiter Beweis. ***D.*** Einer und derselben beliebigen Verbindung der $\nu-1$ Elemente $a, b, c, d, \ldots. m$ kann das νte Element n an ν und nicht an mehreren ***verschiedenen Stellen*** hinzugefügt werden; nemlich, erst ***unmittelbar hinter*** jedem der $\nu-1$ Elemente, und dann noch ***vor*** dem ersten. Die auf solche Weise aus ***einer*** der Verbindungen der $\nu-1$ Elemente entstehenden ν Verbindungen sind alle unter sich verschieden, denn jede hat n an einer ***andern Stelle;*** auch giebt es ihrer nicht mehrere.

E. Was nun von irgend einer der Verbindungen von $\nu-1$ Elementen gilt, gilt auch gleichmäfsig von ***jeder*** andern ihrer sämmtlichen Verbindungen, deren ***Anzahl*** durch $\overset{\nu-1}{x}$ bezeichnet wurde. Jede derselben giebt durch Hinzufügung des neuen, νten Elements n, ν unter sich verschiedene Verbindungen. Auch sind stets die aus den ***verschiedenen*** $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen hervorgehenden Verbindungen von ν Elementen von den vorigen verschieden; denn die $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen sind es ***ehe*** ihnen das neue Element n hinzugefügt wurde, also sind sie es auch noch ***hernach,*** da durch die Hinzufügung von n an der Aufeinanderfolge der $\nu-1$ Elemente $a, b, c, d, \ldots. m$ nichts geändert wird.

F. Die durch die Hinzufügung des νten Elements n entstehenden $\overset{\nu-1}{x}$ Gruppen, jede von ν Verbindungen, und folglich die entstehenden $\overset{\nu-1}{x}.\nu$ Verbindungen sind daher ***sämmtlich*** von einander verschieden. Auch giebt es ***nicht mehrere*** Verbindungen der ν Elemente; denn jeder der $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen kann das νte Element auf nicht mehr als ν Arten hinzugefügt werden (***D.***), und der Verbindungen von $\nu-1$ Elementen, welchen das νte Element hinzugefügt werden könnte, giebt es nach der ***Voraussetzung*** nicht mehr als $\overset{\nu-1}{x}$. Die erlangten Verbindungen von ν Elementen sind also

alle möglichen, deren Anzahl durch $\overset{\nu}{x}$ bezeichnet wurde: folglich ist

$$7.\quad \overset{\nu-1}{x}.\nu = \overset{\nu}{x}.$$

Dieses ist dieselbe Gleichung wie (5. in *B.*), da, wie aus (*B.* §. 4.) erhellet, zwei ganzzahlige Factoren verwechselt werden können, ohne dafs das Product sich änderte. Aus (7.) folgt das Übrige wie in (*C.*).

Anm. Der erste Beweis weiset nach, dafs die möglichen Verbindungen von ν Elementen aus ν Gruppen von $\overset{\nu-1}{x}$ verschiedenen Verbindungen von $\nu-1$ Elementen bestehen: der zweite, dafs sie aus $\overset{\nu-1}{x}$ Gruppen von ν verschiedenen Verbindungen von $\nu-1$ Elementen bestehen; welches die Gleichungen (5.) und (7.) giebt, die nach (*B.* §. 4.) Eines und Dasselbe bedeuten. Aus (5. u. 7.) folgt der Satz, wenn man der Reihe nach $\nu = 2, 3, 4, \ldots \nu$ setzt.

Übrigens ist zu Dem was weiter folgt *nur eine* der beiden Gleichungen (5. u. 7.) nöthig, also eigentlich noch nicht die Zuhülfenahme des in (*B.* §. 4.) sich ergebenden Satzes, dafs in einem Product von *zwei* Factoren die beiden Factoren *verwechselt* werden können.

§. 6.

Lehrsatz.

I. ***Die Ordnung, in welcher die ungleichen oder gleichen ganzzahligen Factoren eines Products, z. B. die ν ganzzahligen Factoren*** a, b, c, d, ... m, n ***des Products***

$$1.\quad \mathrm{P} = \mathrm{a.b.c.d \ldots m.n}$$

aufeinander folgen, kann nach Belieben verändert werden, ohne dafs sich der Werth des Products änderte.

II. ***Die Anzahl*** $\overset{\nu}{\mathrm{x}}$ ***der verschiedenen möglichen Arten, in welchen die Factoren auf einander folgen können, ist***

$$2.\quad \overset{\nu}{\mathrm{x}} = 1.2.3.4.5 \ldots \nu.$$

Beispiel. Alle die

$$3.\quad 1.2.3.4 = 24$$

Producte

$$4.\quad \begin{cases} 2.3.7.9, & 2.7.3.9, & 3.2.7.9, & 3.7.2.9, & 7.2.3.9, & 7.3.2.9, \\ 2.3.9.7, & 2.9.3.7, & 3.2.9.7, & 3.9.2.7, & 9.2.3.7, & 9.3.2.7, \\ 2.9.7.3, & 2.7.9.3, & 9.2.7.3, & 9.7.2.3, & 7.2.9.3, & 7.9.2.3, \\ 9.3.7.2, & 9.7.3.2, & 3.9.7.2, & 3.7.9.2, & 7.9.3.2, & 7.3.9.2 \end{cases}$$

haben sämmtlich denselben Werth 378.

Erster Beweis. *A.* Nach dem Lehrsatze (§. 4.) können die Multiplicationszeichen wo man will *weggelassen* werden, ohne dafs der Werth des Products sich änderte.

Man lasse sie in (1.) *alle bis auf irgend eins*, z. B. bis auf das zwischen g und h, weg, so ist

$$5.\quad P = abcd \ldots g \times hi \ldots lmn.$$

Dieser Ausdruck von P heifst: es soll die *Zahl* $abcd \ldots g$, die durch G bezeichnet werden mag, mit der Zahl $hi \ldots lmn$, welche H sein mag, multiplicirt werden: das Product davon sei P. Es ist also

$$6.\quad P = G.H.$$

B. Die Zahl

$$7.\quad H = hi \ldots lmn \;(A.)$$

ist aber (nach §. 1.) nichts anders als

$$8.\quad H = hi \ldots lm.n:$$

daher ist, wenn man der Kürze wegen die Zahl $hi \ldots lm$ durch M bezeichnet,

$$9.\quad H = M.n.$$

C. Nun schreibe man so viele *Einheiten* in eine horizontale Reihe, als deren die Zahl M enthält, und so viele solcher *Reihen* unter einander, als *Einheiten* in der Zahl n enthalten sind, nemlich wie folgt:

$$10.\quad \left.\begin{matrix} \overbrace{\begin{matrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{matrix}}^{M} \end{matrix}\right\} n.$$

Hier sind offenbar in Allem so viele Einheiten hingeschrieben worden, als das Product $M.n$ und folglich die Zahl H enthält, und man findet ihre Anzahl, wenn man M, wie es sein soll, mit n multiplicirt. Man findet aber auch ihre Anzahl, wenn man n mit M multiplicirt; denn es befinden sich in jeder *verticalen* Reihe n Einheiten (nemlich so viele als horizontale *Reihen*), und solcher *verticalen* Reihen sind M vorhanden (nemlich so viele als *Einheiten* in jeder horizontalen Reihe). Also ist

$$11.\quad M.n = n.M,$$

das heifst, es ist

$$12.\quad hi \ldots lm \times n = n \times hi \ldots lm = H \;(8.).$$

D. Aber zufolge (§. 4.) ist auch, da das Multiplicationszeichen zwischen *n* und *h* weggelassen werden kann,

$$13.\quad n \times hi \ldots . lm = nhi \ldots . lm,$$

also ist auch zufolge (12. und 7.)

$$14.\quad nhi \ldots . lm = hi \ldots . lmn = H,$$

und folglich, vermöge (6.),

$$15.\quad P = G.nhi \ldots . lm = abcd \ldots . g \times nhi \ldots . lm \ (5.)$$

mithin nach (§. 4.) auch

$$16.\quad P = abcd \ldots . gnhi \ldots . lm,$$

und da vermöge (§. 4.) auch

$$17.\quad P = abcd \ldots . ghi \ldots . lmn$$

ist,

$$18.\quad abcd \ldots . gnhi \ldots . lm = abcd \ldots . ghi \ldots . lmn = P,$$

oder auch, da zufolge (§. 4.) $abcd \ldots . gnhi \ldots . lm$ dasselbe ist, wie $a.b.c.d \ldots . g.n.h.i \ldots . l.m$,

$$19.\quad a.b.c.d \ldots . g.n.h.i \ldots . l.m = a.b.c.d \ldots . g.h.i \ldots . l.m.n = P.$$

E. Hieraus folgt, dafs der *letzte* Factor *n* von *P jede beliebige* Stelle einnehmen kann, ohne dafs der Werth von *P* sich änderte; denn, eben so wie er hier zwischen *g* und *h* getreten ist, kann er auch zwischen zwei *beliebige* andere Factoren treten, und selbst vor *alle* ihm vorhergehende Factoren; denn für den letzten Fall darf man sich *P* nur als $1.a.b.c.d \ldots . l.m.n$ vorstellen und *n* zwischen 1 und den Factor *a* treten lassen.

F. Nun setze man für den Augenblick *voraus*, in einem Product von $\nu-1$ Factoren, z. B. in dem Product

$$20.\quad X_1 = a.b.c.d \ldots . l.m,$$

welches also hier

$$21.\quad P = X_1.n = a.b.c.d \ldots . l.m.n$$

giebt, dürfen wirklich *alle* Factoren nach Belieben vertauscht werden, ohne dafs der Werth von X_1 sich änderte, so ändert sich offenbar durch alle diese Vertauschungen auch der Werth von $P = X_1 n$ nicht.

G. Wie oben gezeigt, kann aber der *letzte* Factor *n* in *P* (21.) irgendwo anders hin, also *vor m* treten, ohne dafs dadurch *der Werth von P* sich änderte. Also kann *P* auch durch

$$22.\quad P = X_2.m$$

ausgedrückt werden, wo X_2, eben wie X_1, $\nu-1$ Factoren enthält, und zwar *alle* Factoren von *P* bis auf den *einen m*.

H. Ist nun die Voraussetzung richtig, dafs in einem Product von $\nu-1$ Factoren alle diese Factoren nach Belieben vertauscht werden können, ohne dafs der Werth des Products sich änderte, so können alle diese möglichen Vertauschungen auch in X_2 geschehen, ohne dafs der Werth von X_2 und mithin zufolge (22.) der Werth von P ein anderer würde.

I. Unter den verschiedenen *möglichen* Formen von X_2 werden nothwendig auch solche sein, die l zum *letzten* Factor haben. *Vor* diesen letzten Factor kann, in irgend einer derselben, wieder dem oben Bewiesenen zufolge, in (22.) m treten, ohne dafs P sich änderte: also kann auch P durch

$$23. \quad P = X_3 . l$$

ausgedrückt werden, wo X_3, eben wie X_2 und X_1, $\nu-1$ Factoren enthält; und zwar *alle* Factoren von P bis auf den *einen* l.

K. Hier können abermals, immer insofern die obige Voraussetzung (*F.*) richtig ist, die Factoren in X_3 auf alle mögliche Arten vertauscht werden, ohne dafs der Werth von X_3, und folglich auch ohne dafs P sich ändert.

L. Nimmt man aus den verschiedenen Formen von X_3 eine, in welcher k der *letzte* Factor ist, so kann in (23.) vor k wieder l treten und folglich P auch durch $X_4 . k$ ausgedrückt werden. Und so weiter.

M. Alle die verschiedenen Ausdrücke

$$24. \quad X_1 . n, \; X_2 . m, \; X_3 . l, \; X_4 . k, \; \ldots \; X_\nu a$$

geben also sämmtlich den *gleichen* Werth von P, stets insofern die Voraussetzung richtig ist, dafs in einem Product von $\nu-1$ Factoren die sämmtlichen Factoren nach Belieben vertauscht werden dürfen.

N. Die verschiedenen Ausdrücke (24.) von P enthalten aber, wie aus dem ersten Beweise des Lehrsatzes (§. 5.) hervorgeht, *alle möglichen* Vertauschungen der *sämmtlichen* ν *Factoren von* P. Also folgt bis hieher, dafs, *insofern* es wahr ist, dafs in einem Product von $\nu-1$ Factoren die Factoren auf *alle mögliche* Arten vertauscht werden dürfen, ohne dafs der Werth des Products sich änderte, das *Gleiche* auch für ein Product von ν Factoren gilt.

O. In einem Product von zwei Factoren, z. B. a und b, dürfen aber wirklich die beiden Factoren auf die für sie *möglichen zwei* Arten vertauscht werden, ohne dafs der Werth des Productes sich ändert. Dieses folgt aus (*C.*): denn so wie dort $M.n = n.M$ ist (11.), so ist auch $a.b = b.a$.

Also folgt aus (*N.*), dafs auch in einem Product von 3 Factoren die

D. Aber zufolge (§. 4.) ist auch, da das Multiplicationszeichen zwischen *n* und *h* weggelassen werden kann,

$$13.\quad n \times hi \ldots . lm = nhi \ldots . lm,$$

also ist auch zufolge (12. und 7.)

$$14.\quad nhi \ldots . lm = hi \ldots . lmn = H,$$

und folglich, vermöge (6.),

$$15.\quad P = G.nhi \ldots . lm = abcd \ldots . g \times nhi \ldots . lm \; (5.);$$

mithin nach (§. 4.) auch

$$16.\quad P = abcd \ldots . gnhi \ldots . lm;$$

und da vermöge (§. 4.) auch

$$17.\quad P = abcd \ldots . ghi \ldots . lmn$$

ist,

$$18.\quad abcd \ldots . gnhi \ldots . lm = abcd \ldots . ghi \ldots . lmn = P,$$

oder auch, da zufolge (§. 4.) $abcd \ldots . gnhi \ldots . lm$ dasselbe ist, wie $a.b.c.d \ldots . g.n.h.i \ldots . l.m$,

$$19.\quad a.b.c.d \ldots . g.n.h.i \ldots . l.m = a.b.c.d \ldots . g.h.i \ldots . l.m.n = P.$$

E. Hieraus folgt, dafs der *letzte* Factor *n* von *P jede beliebige* Stelle einnehmen kann, ohne dafs der Werth von *P* sich änderte; denn, eben so wie er hier zwischen *g* und *h* getreten ist, kann er auch zwischen zwei *beliebige* andere Factoren treten, und selbst vor *alle* ihm vorhergehende Factoren; denn für den letzten Fall darf man sich *P* nur als $1.a.b.c.d \ldots . l.m.n$ vorstellen und *n* zwischen 1 und den Factor *a* treten lassen.

F. Nun setze man für den Augenblick *voraus*, in einem Product von $\nu - 1$ Factoren, z. B. in dem Product

$$20.\quad X_1 = a.b.c.d \ldots . l.m,$$

welches also hier

$$21.\quad P = X_1.n = a.b.c.d \ldots . l.m.n$$

giebt, dürfen wirklich *alle* Factoren nach Belieben vertauscht werden, ohne dafs der Werth von X_1 sich änderte, so ändert sich offenbar durch alle diese Vertauschungen auch der Werth von $P = X_1 n$ nicht.

G. Wie oben gezeigt, kann aber der *letzte* Factor *n* in *P* (21.) irgendwo anders hin, also *vor m* treten, ohne dafs dadurch *der Werth von P* sich änderte. Also kann *P* auch durch

$$22.\quad P = X_2.m$$

ausgedrückt werden, wo X_2, eben wie X_1, $\nu - 1$ Factoren enthält, und zwar *alle* Factoren von *P* bis auf den *einen m*.

H. Ist nun die Voraussetzung richtig, dafs in einem Product von $\nu-1$ Factoren alle diese Factoren nach Belieben vertauscht werden können, ohne dafs der Werth des Products sich änderte, so können alle diese möglichen Vertauschungen auch in X_2 geschehen, ohne dafs der Werth von X_2 und mithin zufolge (22.) der Werth von P ein anderer würde.

I. Unter den verschiedenen *möglichen* Formen von X_2 werden nothwendig auch solche sein, die l zum *letzten* Factor haben. *Vor* diesen letzten Factor kann, in irgend einer derselben, wieder dem oben Bewiesenen zufolge, in (22.) m treten, ohne dafs P sich änderte: also kann auch P durch

$$23. \quad P = X_3 . l$$

ausgedrückt werden, wo X_3, eben wie X_2 und X_1, $\nu-1$ Factoren enthält; und zwar *alle* Factoren von P bis auf den *einen* l.

K. Hier können abermals, immer insofern die obige Voraussetzung (*F.*) richtig ist, die Factoren in X_3 auf alle mögliche Arten vertauscht werden, ohne dafs der Werth von X_3, und folglich auch ohne dafs P sich ändert.

L. Nimmt man aus den verschiedenen Formen von X_3 eine, in welcher k der *letzte* Factor ist, so kann in (23.) vor k wieder l treten und folglich P auch durch $X_4 . k$ ausgedrückt werden. Und so weiter.

M. Alle die verschiedenen Ausdrücke

$$24. \quad X_1 . n, \quad X_2 . m, \quad X_3 . l, \quad X_4 . k, \ldots X_\nu . a$$

geben also sämmtlich den *gleichen* Werth von P, stets insofern die Voraussetzung richtig ist, dafs in einem Product von $\nu-1$ Factoren die sämmtlichen Factoren nach Belieben vertauscht werden dürfen.

N. Die verschiedenen Ausdrücke (24.) von P enthalten aber, wie aus dem ersten Beweise des Lehrsatzes (§. 5.) hervorgeht, *alle möglichen* Vertauschungen der *sämmtlichen* ν *Factoren von P*. Also folgt bis hieher, dafs, *insofern* es wahr ist, dafs in einem Product von $\nu-1$ Factoren die Factoren auf *alle mögliche* Arten vertauscht werden dürfen, ohne dafs der Werth des Products sich änderte, das *Gleiche* auch für ein Product von ν Factoren gilt.

O. In einem Product von zwei Factoren, z. B. a und b, dürfen aber wirklich die beiden Factoren auf die für sie *möglichen zwei* Arten vertauscht werden, ohne dafs der Werth des Productes sich ändert. Dieses folgt aus (*C.*): denn so wie dort $M . n = n . M$ ist (11.), so ist auch $a . b = b . a$.

Also folgt aus (*N.*), dafs auch in einem Product von 3 Factoren die

Factoren auf alle mögliche Arten vertauscht werden dürfen, und folglich auch in Producten von 4, 5, 6 u. s. w. Factoren; was zu beweisen war.

P. Die Zahl der möglichen Vertauschungen von ν Factoren ist, wie unmittelbar aus dem Lehrsatz (5.) hervorgeht, $x_\nu = 1.2.3.4 \ldots \nu$; wie es (2.) ausdrückt.

Anm. Die Hauptpuncte dieses Beweises sind, dafs erstlich der *letzte* Factor eines Products seine Stelle mit jedem vorhergehenden vertauschen kann; sodann, dafs, insofern die $\nu-1$ Factoren eines Products nach Belieben vertauscht werden dürfen, jeder der ν Factoren zum *letzten* gemacht werden kann, dafs auf solche Weise *alle möglichen* Vertauschungen von ν Factoren erlangt werden, und dann, dafs die vorausgesetzte Zuläfslichkeit der Vertauschung der Factoren für *zwei* Factoren *wirklich* stattfindet. Der Beweis stützt sich auf die Lehrsätze (§. 4. u. 5.).

Zweiter Beweis. **Q.** Man setze, wie oben in (*F.*), einen Augenblick voraus, es dürfen in dem Product von $\nu-1$ Factoren

$$25. \quad X_1 = abcd \ldots lm$$

die Factoren auf alle möglichen Arten vertauscht werden, ohne dafs der Werth des Products sich änderte. Ist diese Voraussetzung richtig, so wird der Werth des Productes

$$26. \quad P = X_1.n = abcd \ldots lm.n$$

von ν Factoren sich nicht ändern, wie man auch in X_1 die $\nu-1$ Factoren $a, b, c, d, \ldots m$ versetzen mag.

R. Nun ist P (26.) nach (§. 1.) nichts anderes als

$$27. \quad P = L.m.n,$$

wenn man das Product $abcd \ldots l$ durch L bezeichnet; das heifst, es mufs L erst mmal und das was herauskommt nmal genommen werden.

S. Auf dieselbe Weise, wie in (*B.* §. 4.), folgt aber, dafs $L.m.n$ nichts anders als $L.mn$, also auch

$$28. \quad P = L.mn$$

ist, das heifst, dafs man P auch findet, wenn man L *sogleich* mit der Zahl mn multiplicirt, die das Product von m und n ist.

T. Ferner folgt auf dieselbe Weise wie oben in (*C.*), dafs $mn = nm$ ist. Mithin ist auch

$$29. \quad P = L.nm.$$

Und da nach (§. 4. *B.*) auch $L.n.m = L.nm$ ist, so folgt, dafs auch

$$30. \quad P = L.n.m,$$

das heifst

$$31. \quad P = abcd \ldots . \, l.n.m$$

oder auch nach (§. 1.)

$$32. \quad P = abcd \ldots . \, ln.m$$

ist, was der Kürze wegen durch

$$33. \quad P = X_2.m$$

bezeichnet werden mag.

Von hier ab weiter ist der Beweis im Wesentlichen derselbe wie der Theil (*H.* bis *P.*) des ersten Beweises.

Anm. Dieser zweite Beweis bedarf nicht des vollständigen Lehrsatzes (§. 4.). Er nimmt daraus nur was ihm nöthig ist, nemlich den Theil (*B.*). Der vollständige Satz (§. 4.) kann indessen in andern Fällen Anwendung finden.

Dritter Beweis. *U.* Das Product

$$34. \quad P_\nu = (1+a)(1+b)(1+c)(1+d) \ldots (1+n)$$

enthält, wenn man die angedeuteten Multiplicationen ausführt, zufolge (§. 2.) nächst der Einheit *alle möglichen* Producte von a, b, c, d, ... n zu einem, zwei, drei, vier u. s. w. bis ν Factoren. Zum Beispiel

$$35. \quad (1+a)(1+b)(1+c)(1+d) = 1 + a + b + c + d + ab + ac + ad + bc + bd + cd + abc + abd + acd + bcd + abcd.$$

V. Man *setze einen Augenblick voraus,* dafs in einem Product von ν Factoren a, b, c, d, ... n, also auch von *weniger* als ν Factoren, die Factoren nach Belieben vertauscht werden können, ohne dafs der *Werth* des Products sich änderte.

W. Nun vertausche man z. B. in (35.) *rechterhand* die Factoren a, b, c, d der einzelnen Glieder nach Belieben wirklich, so werden dadurch weder *mehr* Glieder, noch Glieder entstehen können, die *andere* Factoren enthielten als die vorigen; denn es sind von jeder *Art* von Gliedern, zu einem, zwei, drei und vier Factoren, wie §. 2. *beweiset,* immer *alle möglichen* vorhanden. Die Glieder, welche man durch die Vertauschung erhält, werden von den vorigen in sich durch nichts weiter als durch die verschiedene Aufeinanderfolge ihrer Factoren verschieden sein. Dadurch ändert sich aber *nach der Voraussetzung* ihr Werth nicht, also auch nicht die Summe der Glie-

der, und folglich auch der Werth z. B. von $(1+a)(1+b)(1+c)(1+d)$ in (35.) nicht.

Die Vertauschung von a, b, c und d in (35.) bringt aber *linkerhand* nichts anderes hervor, als die Vertauschung der Factoren $1+a$, $1+b$, $1+c$, $1+d$ *selbst;* also folgt bis hierher, dafs, wenn die Voraussetzung: es ändere sich der Werth eines Productes von ν und weniger Factoren (hier in dem Beispiel von 4 Factoren) durch die Vertauschung der Factoren nicht, *für die Werthe* $a, b, c, d, \ldots$ der Factoren richtig ist, dasselbe auch für die *um 1 gröfseren Werthe* $1+a$, $1+b$, $1+c$, $1+d$, ... der Factoren gilt.

X. Daraus folgt weiter, dafs die Voraussetzung für die Werthe $a, b, c, d, \ldots$ der Factoren gilt, wenn sie für die um 1 *kleineren* Werthe $a-1$, $b-1$, $c-1$, $d-1$, ... derselben stattfindet, also ferner, auch schon, wenn sie für die Werthe $a-2$, $b-2$, $c-2$, $d-2$, ... gilt, und so weiter: also auch dann schon, wenn sie, im Fall etwa a der *kleinste* der Factoren ist, für die Werthe 1, $b-(a-1)$, $c-(a-1)$, $d-(a-1)$, ..., mithin *blofs für $\nu-1$ Factoren* gilt; denn 1 hat als Factor keine Wirkung.

Y. Der *vorausgesetzte* Satz, dafs die Factoren eines Products nach Belieben vertauscht werden können, gilt also für ν beliebige Factoren schon dann, wenn er für $\nu-1$ beliebige Factoren gilt. Daraus folgt, dafs er für $\nu-1$ Factoren, also auch für ν Factoren gilt, wenn er für $\nu-2$ Factoren stattfindet u. s. w.: zuletzt also blofs, wenn z. B. $1.a = a.1$ ist. Dies aber ist offenbar der Fall: also gilt der Satz, dafs sich der Werth eines Products beliebiger Factoren durch die Versetzung derselben nicht ändert, wirklich; was zu beweisen war.

Anm. Dieser Beweis stützt sich *blofs* auf den Lehrsatz (§. 2.).

Anm. zu §. 2. bis 6. Man wolle an die scheinbar zu viele Allgemeinheit und Abstraction, so wie an die scheinbar zu grofse Zurüstung für so einfache Dinge wie die vorhergehenden, von welchen sich schon durch blofse Anschauung eine Überzeugung (freilich dann nur eine Art von Überzeugung) erlangen läfst, nicht Anstofs nehmen. Die Übung des Lernenden im Denken, Schliefsen und Urtheilen, also auch in der Abstraction, ist einer der *Zwecke* der gegenwärtigen Schrift. Die Zurüstung für den gegenwärtigen Hauptsatz §. 6., in den vorhergehenden, dürfte, wenn man vollkommene *Strenge* verlangt, nöthig sein. Die Beweise No. 1. und 2. §. 6. dürften sich nicht wohl kürzer und nicht ohne die vorhergehenden Sätze mit *gleicher Strenge* geben lassen.

§. 7.

Lehrsatz.

Die Vorzeichen + und − von ν Factoren a, b, c, d, ... n *eines Products*

$$1.\quad P = abcd \ldots n$$

können auf

$$2.\quad 2^{\nu-1}$$

Arten verändert werden, ohne daſs das Vorzeichen des Products sich änderte.

Beispiel. Für $\nu = 4$ ist

$$3.\quad +P$$

$$= +a.+b.+c.+d = +a.+b.-c.-d = +a.-b.+c.-d = -a.+b.+c.-d$$
$$= +a.-b.-c.+d = -a.+b.-c.+d = -a.-b.+c.+d = -a.-b.-c.-d$$

und

$$4.\quad -P$$

$$= +a.+b.+c.-d = +a.+b.-c.+d = +a.-b.+c.+d = -a.+b.+c.+d$$
$$= +a.-b.-c.-d = -a.+b.-c.-d = -a.-b.+c.-d = -a.-b.-c.+d;$$

und mehr als diese $2^{\nu-1} = 2^3 = 8$ Veränderungen der Zeichen sind für $+P$, so wie für $-P$, nicht möglich.

Beweis. *A.* Es sei für $\varkappa < \nu$ Factoren $a, b, c, d, \ldots k$

$$5.\quad a.b.c.d \ldots k = K,$$

und für die $\varkappa + 1$ Factoren $a, b, c, d, \ldots k, l$,

$$6.\quad a.b.c.d \ldots k.l = l.K = L.$$

B. In dem Product der zwei Factoren l und K, nemlich in

$$7.\quad l.K = L$$

können offenbar die Vorzeichen von l und K nur auf **2** *verschiedene* Arten verändert werden, ohne daſs das Vorzeichen von L sich änderte. Nemlich es ist nur

$$8.\quad +L = +K.+l = -K.-l \text{ und}$$

$$9.\quad -L = +K.-l = -K.+l.$$

C. Nun setze man, in dem Product K von $\varkappa$ Factoren können die Vorzeichen der Factoren $x_\varkappa$ *mal* verändert werden, ohne daſs das Vorzeichen von K sich änderte. Alsdann folgt aus (8. u. 9.), daſs in dem Product L von $\varkappa+1$ Factoren die Vorzeichen der Factoren $2x_\varkappa$ *mal* verändert werden können, ohne daſs das Vorzeichen von L sich änderte. Dieses gilt für *jeden* Werth von $\varkappa$, von 2 an, so weit man will.

D. Es können aber, wie ebenfalls aus (8. u. 9.) folgt, wenn man sich unter *K* nur einen einfachen Factor vorstellt, für $\varkappa = 2$ Factoren die Vorzeichen der Factoren auf 2 verschiedene Arten verändert werden, ohne daſs das Vorzeichen des Products sich änderte; also ist solches für $\varkappa = 3$ Factoren auf $2.2 = 2^2$, für $\varkappa = 4$ Factoren auf $2.2^2 = 2^3$, für $\varkappa = 5$ Factoren auf $2.2^3 = 2^4$ u. s. w. und allgemein für $\varkappa = \nu$ Factoren auf $2^{\nu-1}$ Arten möglich; wie es der Lehrsatz behauptet.

§. 8.

Erklärungen.

I. Insbesondere bei *ganzen* Zahlen kann man im Allgemeinen diejenige Zahl ***Rest*** nennen, welche entsteht, wenn mit irgend einer Zahl z ein Vielfaches, z. B. das qfache einer andern Zahl u durch das Minuszeichen verbunden wird. Desgleichen kann im Allgemeinen jene ***Anzahl*** des Vielfachen von u ***Quotient*** heiſsen, die Zahl z ***Dividend***, und die Zahl u ***Divisor***, so daſs in der Gleichung

$$1. \quad z - qu = r \quad \text{oder} \quad z = qu + r$$

z der ***Dividend***, u der ***Divisor***, q der ***Quotient*** und r der ***Rest*** ist.

Der ***Quotient*** q ist allgemein *ganz willkürlich*, und kann z. B. jede beliebige *positive ganze* Zahl sein, also $= 0, 1, 2, 3, 4, \ldots$, bis ins Unendliche. Er könnte selbst jede beliebige *negative ganze* Zahl sein; allein dann pflegt man r nicht mehr ***Rest***, sondern ***Summe*** zu nennen.

II. Zu *jedem* beliebigen Werth von q gehört vermöge der Gleichung (1.) natürlich *ein*, und *nur ein* Werth von r; also zu jedem *andern* Werth von q ein anderer Werth von r, und es giebt folglich eben so viele Werthe von r, als von q; mithin *unzählige*. Zu jedem Werth von r gehört umgekehrt ein Werth von q, und *nur einer*. Die Werthe von r können *positiv*, *null* und *negativ* sein. Sie sind *positiv* so lange $qu < z$, *negativ* wenn $qu > z$, und null wenn $qu = z$ ist. Letzteres ist der Fall, wenn u in z *aufgeht;* und *nur dann*.

III. *a.* Die Anzahl der *positiven* r ist für positive z, q und u immer *begrenzt*. Es giebt ihrer so viele als Werthe von q, für welche qu nicht gröſser als z ist. Wenigstens *einen* positiven Werth von r aber giebt es auch für positive q *immer*, selbst wenn $z < u$ ist; in welchem Fall er zu $q = 0$ gehört und z selbst ist. Ist $z > u$, so kann es der positiven Werthe von r, die kleiner als u sind, mehrere geben.

b. Die Anzahl der *negativen* Werthe von r ist immer *unendlich grofs.* Alle r sind negativ, die zu positiven Werthen von q gehören, für welche $qu > z$ ist; und solcher Werthe von q giebt es unzählige, da q ohne Ende wachsen kann.

c. Der Werth 0 von r kommt für *ganzzahlige* q, wie schon bemerkt, nur dann vor, wenn u in z *aufgeht.* Verlangt man aber den Werth 0 von r auch in dem Fall, wenn u in z *nicht aufgeht,* so bekommt der Quotient $q = \frac{z}{u}$ keine *ganze* Zahl zum Werthe. Er ist alsdann ein ***Bruch.*** Geht u in z auf, so kann man den Quotienten zur Unterscheidung *ganzzahlig* nennen. Der ***Bruch*** $\frac{z}{u}$ heifst *unecht,* wenn $z > u$, *echt,* wenn $z < u$ ist.

IV. Da die Werthe, welche der Rest r haben kann, alle von einander verschieden sind, nemlich jeder von dem nächsten um u, so wie q um 1 wächst oder abnimmt, so wird es nothwendig immer, sowohl unter den positiven als unter den negativen Werthen von r, *einen* und *nur einen* geben, der, abgesehen vom Zeichen, durch eine *kleinere Zahl* ausgedrückt ist, als alle übrigen *seiner Art.*

Da nun in Dem, was weiter folgt, die beiden Reste r, die unter allen übrigen ihrer Art die *kleinsten* Zahlenwerthe haben, *insbesondere* in Betracht kommen, so wird es gut sein, ihnen, nebst den ihnen correspondirenden Quotienten für *ganze* Zahlen, eine ausschliefsliche abgekürzte ***Benennung*** zu geben.

a. Es sollen die beiden Reste, welche die *kleinsten* Zahlenwerthe haben, *echte* Reste heifsen; und zwar derjenige mit dem Pluszeichen ***positiver echter Rest,*** der mit dem Minuszeichen ***negativer echter Rest.*** Derjenige von beiden, welcher, falls die beiden Reste ungleich sind, abgesehen vom Zeichen, den *kleinsten* Zahlenwerth hat, und der also dann von *allen möglichen* Resten den kleinsten Zahlenwerth hat, soll ***zeichenfrei-*** oder ***unbedingt echter Rest,*** oder auch blofs ***kleinster Rest*** heifsen; gleichviel ob er positiv oder negativ sei.

b. Die zu den beiden echten Resten gehörigen ***Quotienten*** sollen, um sie von dem Quotienten $\frac{z}{u}$ selbst, den man, er mag eine ganze Zahl oder ein Bruch sein, ***genauen Quotienten*** nennen kann, zu unterscheiden, ***nächste Quotienten*** heifsen; und zwar soll der zu dem *positiven* echten Rest gehörige Quotient ***unternächster Quotient,*** der zu dem *negativen* echten Rest gehörige Quotient ***übernächster Quotient*** genannt werden. Derjenige

von diesen beiden Quotienten, welcher dem *unbedingt nächsten* oder *kleinsten* Rest angehört, soll *unbedingt nächster Quotient* heifsen. Die Ursach der Wahl dieser Benennungen wird sich im folgenden Paragraphen zeigen.

Um die *nächsten* Quotienten, mit Anzeige des Dividenden und Divisors, von dem *genauen* Quotienten zu unterscheiden, welchem die gewöhnliche Bezeichnung $z:u$ oder $\frac{z}{u}$ vorbehalten bleibt, soll der *unternächste Quotient* durch $(z+:u)$, der *übernächste Quotient* durch $(z-;u)$ und der *unbedingt nächste* Quotient durch $[z:u]$ bezeichnet werden.

Beispiele. *No. 1.* Der Dividend z sei $=33$, der Divisor $u=11$, so giebt die Gleichung (1.)

$$2.\quad 33=0.11+33=1.11+22=2.11+11=3.11+0=4.11-11$$
$$=5.11-22\ldots.$$

Hier sind der *positive*, der *negative* und der *unbedingt nächste Rest* alle drei Null. Der *übernächste*, der *unternächste* und der *unbedingt nächste* Quotient sind alle drei $=3$. Der *genaue* Quotient ist gleichfalls $=3$, also *ganzzahlig;* folglich ist hier $(z+:u)=(z-:u)=[z:u]=z:u=\frac{z}{u}$.

No. 2. Der Dividend z sei wieder $=33$, aber der Divisor $u=7$, so ist

$$3.\quad 33=0.7+33=1.7+26=2.7+19=3.7+12=4.7+5=5.7-2$$
$$=6.7-9=7.7-16\ldots.$$

Hier ist der *positive echte* Rest $=+5$, der *negative echte* Rest $=-2$, der *unbedingt echte* Rest $=-2$. Der *unternächste Quotient* $(z+:u)$ ist $=4$, der *übernächste Quotient* $(z-:u)=5$, der *unbedingt nächste Quotient* $[z:u]=5$, der *genaue Quotient* $z:u$ oder $\frac{z}{u}=\frac{33}{7}$, also ein *Bruch,* und zwar ein *unechter* Bruch.

No. 3. Der Dividend z sei abermals $=33$, der Divisor $u=41$, so ist

$$4.\quad 33=0.41+33=1.41-8=2.41-49=3.41-90\ldots.$$

Hier ist der *positive echte Rest* $=+33$, der *negative echte* Rest $=-8$, der *unbedingt echte* Rest $=-8$. Der *unternächste Quotient* $(z+:u)$ ist $=0$, der *übernächste Quotient* $(z-:u)=1$, der *unbedingt nächste* Quotient $[z:u]=1$. Der genaue Quotient $z:u$ oder $\frac{z}{u}$ ist $=\frac{33}{41}$, also ein *Bruch,* und zwar ein *echter* Bruch.

§. 9.

Erläuterungen zum vorigen Paragraphen.

I. Wenn der Divisor u in den Dividenden z *aufgeht*, so ist immer

$$1. \quad (z+:u) = (z-:u) = [z:u] = z:u = \frac{z}{u}.$$

Der *negative*, der *positive* und der *unbedingt echte Rest* sind alle drei Null, und der *unternächste*, der *übernächste* und der *genaue* Quotient sind einander *gleich* und *ganze* Zahlen. Dieses ist an sich klar, und das Beispiel (No. 1. §. 8.) macht es anschaulich.

II. Wenn der Divisor u in den Dividenden z nicht *aufgeht*, so sind die *absoluten Zahlenwerthe* oder, wie man füglich auf deutsch sie nennen kann, die *zeichenfreien Zahlenwerthe* beider echten Reste nothwendig unter den Zahlen

$$2. \quad 1,\ 2,\ 3,\ 4, \ldots u-1$$

anzutreffen. Denn wenn man, der Gleichung

$$3. \quad z-qu = r \quad (§. 8.\ 1.)$$

gemäfs, u von z so oft *als möglich* abzieht, so kann das r, welches bleibt, nicht mehr *gröfser* als u sein; auch, in dem Fall, wenn z mit u *nicht* aufgeht, weder u noch 0. Also kann der *positive echte* Rest nur eine der Zahlen (2.) sein. Zieht man u noch weiter ab, so kann der nächste Rest, welches der negative echte Rest ist, weder $<-u$, noch 0, noch $-u$ sein, also wiederum nur eine der Zahlen (2.), mit dem Minuszeichen.

Ganz eben so verhält es sich, wenn z und u beide *negativ* sind, denn dann heifst die Gleichung (3.)

$$4. \quad \begin{cases} -z+qu = -r \text{ oder} \\ -(z-qu) = -r. \end{cases}$$

Auch in diesem Fall sind die absoluten Zahlenwerthe beider echten Reste nothwendig unter den Zahlen (2.) anzutreffen.

III. Der *algebraische* Werth des *positiven echten* Restes ist immer um den *Divisor* gröfser, als der *algebraische* Werth des *negativen echten* Restes; und von den *zeichenfreien* Zahlenwerthen der beiden Reste ist die *Summe* immer dem Divisor gleich.

Denn den *negativen echten* Rest, welcher durch $-\varrho$ bezeichnet werden mag, erhält man aus dem *positiven echten* Rest, welcher $+r$ sein mag, wenn man den Divisor u von $+r$ noch einmal abzieht, so dafs also $+r-u = -\varrho$ ist: mithin ist $+r$ um u gröfser als $-\varrho$. Ferner folgt aus $+r-u$

$= -\varrho$, $+r+\varrho = +u$, und folglich ist die Summe der ***zeichenfreien*** Zahlenwerthe r und ϱ der beiden Reste dem Divisor u gleich.

IV. Der Zahlenwerth des ***unbedingt echten*** Restes kann nicht gröfser als ***die Hälfte des Divisors*** sein.

Denn da die absoluten Zahlenwerthe r und ϱ der beiden echten Reste zufolge (III.) u ausmachen, so können nicht beide zugleich gröfser als $\frac{1}{2}u$ sein; sonst wäre $+r+\varrho > u$, nicht $= u$. Also können r und ϱ nur entweder beide $= \frac{1}{2}u$ sein, oder derjenige, welcher von beiden der kleinere und welcher dann der ***unbedingt echte Rest*** ist, mufs $< \frac{1}{2}u$ sein. In ***keinem*** Falle also ist der ***unbedingt echte*** Rest ***gröfser*** als $\frac{1}{2}u$.

Auch verhält es sich ganz so, wenn z und u beide ***negativ*** sind.

V. Die ***zeichenfreien Zahlenwerthe*** r und ϱ des positiven und des negativen echten Restes können nur dann ***einander gleich*** sein, wenn der Divisor u durch 2 theilbar ist; jedoch sind sie es dann nicht nothwendig. Sie sind aber nothwendig ***einander nicht gleich,*** wenn der Divisor u nicht mit 2 aufgeht, was auch der Dividend z sein mag.

Denn da immer $r+\varrho = u$ ist, so ist für $r = \varrho$, $u = 2r = 2\varrho$: also mufs, wenn $r = \varrho$ sein soll, u nothwendig mit 2 aufgehen. Jedoch kann u mit 2 aufgehen, ohne dafs $r = \varrho$ ist; denn in $r+\varrho = u$ kann r mit 2 dividirt den Rest 1 lassen, und ϱ ebenfalls, $r+\varrho$ also den Rest 2, und also kann $r+\varrho = u$ sein, ohne dafs $r = \varrho$ wäre. Ferner kann nicht $r = \varrho$ sein, wenn u ***nicht*** mit 2 aufgeht; denn $r+\varrho = u$ giebt für $r = \varrho$, $u = 2r = 2\varrho$, welches immer mit 2 aufgeht.

VI. Der ***unternächste Quotient,*** zu dem ***positiven*** echten Rest gehörig, ist immer um einen ***echten*** Bruch oder um weniger denn 1 ***kleiner;*** und der ***übernächste Quotient,*** zu dem negativen echten Rest gehörig, ist immer um einen ***echten*** Bruch oder um weniger als 1 ***gröfser,*** als der ***genaue*** Quotient; so dafs es also keine ***ganze*** Zahlen giebt, die dem ***genauen*** Quotienten ***näher kämen,*** als die jener beiden Quotienten. Dieser Umstand ist daraus klar, dafs man von dem positiven unmittelbar zu dem negativen echten Rest gelangt, wenn man den Divisor von ersterem noch ***einmal*** abzieht, während der genaue Quotient ***zwischen*** dem unternächsten und dem übernächsten Quotienten liegt. Dieser Umstand ist der ***Grund,*** weshalb wir die beiden Quotienten ***nächste*** nannten, und zwar den zu dem echten ***positiven*** Rest gehörigen Quotienten ***unternächsten,*** den zu dem echten ***negativen*** Rest gehörigen Quotienten ***übernächsten*** Quotienten, indem ersterer immer ***kleiner,*** letzterer immer ***gröfser*** ist, als der ***genaue*** Quotient.

VII. Der *übernächste* Quotient ist immer um 1 gröfser, als der *unternächste.*

VIII. Kein *Bruch,* z. B. $\frac{z}{u}$, kann einer *ganzen* Zahl gleich sein.

Denn $\frac{z}{u}$ ist dann ein *Bruch,* wenn man durch wiederholtes Abziehen des Divisors u von z *nicht* auf den Rest 0 kommt (§. 8. III. *c.*), sondern auf einen positiven echten Rest r, der > 0 und $< u$ ist. Also ist dann in der Gleichung

$$4.\quad z = qu + r$$

$r > 0$ und $< u$. Dividirt man diese Gleichung mit u, so folgt, dafs der *genaue* Quotient

$$5.\quad \frac{z}{u} = q + \frac{r}{u},$$

das heifst gleich der Summe einer *ganzen* Zahl q und des Bruchs $\frac{r}{u}$ ist, der > 0 und < 1 ist. Er ist also weder die ganze Zahl q, noch die ganze Zahl $q+1$, noch weniger eine andere ganze Zahl, also überhaupt *keine* ganze Zahl.

§. 10.

Erklärungen und Erläuterungen.

I. In der Gleichung

$$1.\quad z = qu + r,$$

in welcher z der *Dividend,* u der *Divisor,* q der *Quotient,* r der *Rest* und q *willkürlich* ist, wenn z und u gegeben sind, kommt es, wenn z und u *ganze* Zahlen sind, um für r ebenfalls eine *ganze* Zahl zu haben, wie schon oben bemerkt, nicht darauf an, dafs q eine ganze *positive* Zahl sei: es kann q auch jede beliebige *negative* ganze Zahl sein. r ist *immer* eine ganze Zahl, welche positive oder negative ganze Zahl auch q sein mag: denn aus (1.) folgt $r = z - qu$, und wenn z, q und u ganze Zahlen sind, so ist auch $z - qu$ eine ganze Zahl, und also auch r, da ein *Bruch* nie einer ganzen Zahl gleich sein kann (§. 9. VIII.).

II. Die Zerlegung einer ganzen Zahl z in irgend ein Vielfaches qu einer andern ganzen Zahl u und in einen Rest r, nach (1.), so dafs man z als die *algebraische* Summe jenes Vielfachen und des Restes betrachtet, findet in der gesammten Theorie der Zahlen unzählige Anwendungen. Diese Zerlegung ist sogar eines der *Hauptmittel,* durch welches diese Theorie zu vielen, selbst fast zu den meisten ihrer Sätze gelangt; denn sie findet solche

häufig durch die Untersuchung Dessen, was bei dieser oder jener Verbindung von Zahlen z, die ***Reste*** derselben r in Beziehung auf andere Zahlen u geben. Schon z. B. die Theilbarkeit oder Nicht-Theilbarkeit einer Zahl z durch u hangt blofs davon ab, ob unter den verschiedenen Werthen, welche der Rest r haben kann, auch der Werth Null ist, oder nicht.

III. Es kommt nun aber bei sehr vielen Untersuchungen, die Eigenschaften der Zahlen betreffend, auf die ***Gröfse*** des Quotienten q ganz und gar nicht an, sondern nur auf die ***Gröfse des Restes*** r allein, und rücksichtlich des ***Quotienten*** einzig und allein ***darauf***, dafs er eine ***ganze*** Zahl sei. Zum Beispiel wenn $z_1, z_2, z_3, \ldots z_n$ mehrere verschiedene ganze Zahlen wären, von welchen irgend eine ***Verbindung*** in Beziehung auf eine andere ganze Zahl u untersucht werden soll, und es wäre etwa

$$2.\quad \begin{cases} z_1 = q_1 u + r_1, \\ z_2 = q_2 u + r_2, \\ z_3 = q_3 u + r_2, \\ \ldots\ldots\ldots \\ z_n = q_n u + r_n, \end{cases}$$

so kann es sein, dafs sich diese Untersuchung schon durch diejenige der ***gleichen*** Verbindung der ***Reste*** r, etwa der positiven oder negativen ***echten*** Reste, oder auch der ***unbedingt echten*** Reste, ***allein*** ausführen läfst und dafs dabei die ***Gröfse*** der Quotienten q ***ganz gleichgültig*** ist. Es ist dies immer der Fall, wenn die ***Resultate dieselben*** bleiben, ***welche*** ganzzahligen Werthe auch die Quotienten q haben mögen; was, wie sich in der Folge zeigen wird, sehr häufig vorkommt. Wo es so ist, entsteht dann offenbar schon der Gewinn, dafs man es statt mit den Zahlen z, die ***sehr grofs*** sein können, nur mit den Resten r, die, wenn man die ***echten*** Reste nimmt, immer ***kleiner als*** u sind, also vielleicht nur noch mit ***viel*** kleineren Zahlen zu thun hat; was indessen häufig noch der geringste Gewinn ist.

IV. Es kann also, wie gesagt, sein, dafs es auf die ***Gröfse*** z. B. ganzzahliger Quotienten q bei dem Ausdruck von Zahlen z, als Summen von Vielfachen einer andern Zahl u und eines Restes, so wie auch zu noch anderen Zwecken, auf die ***Gröfse*** dieser oder jener ganzen Zahlen überhaupt ***gar nicht*** ankommt, sondern nur allein darauf, dafs angezeigt werde, die Quotienten, oder sonst jene Zahlen, ***seien ganze Zahlen.***

In solchen Fällen würde es offenbar unnütz sein, die verschiedenen Quotienten oder Zahlen durch ***verschiedene*** Buchstaben oder Zeichen zu ***unter-***

scheiden. Es geschieht schon Alles, was nöthig ist, wenn man irgend ein *ausschliefsliches* Zeichen blofs *für den Begriff der ganzen Zahl* hat: ein Zeichen, welches blofs *das* ausdrückt, was die drei Worte „*eine ganze Zahl*" aussagen, ohne alle Rücksicht auf die *Gröfse* der Zahl. Es geschieht dann das Nöthige, wenn man dieses Zeichen *ohne alle weitere Unterscheidung* z. B. an die Stelle der verschiedenen Quotienten, oder anderer Zahlen setzt, von welchen nichts weiter ausgesagt werden *soll,* als dafs sie *ganze* Zahlen, nicht Brüche, irrationale Zahlen u. s. w. sind.

V. Da ein *Zeichen* an sich *willkürlich* ist, so könnte man, um den blofsen Begriff der ganzen Zahl z. B. bei den Quotienten auszudrücken, etwa des Buchstabens q oder Q sich bedienen. Allein dies Zeichen wäre nicht allgemein und nicht *ausschliefslich* genug, indem man zu sehr gewohnt ist, unter Buchstaben, die auch noch *anderswo* vorkommen können, einen oder mehrere auf irgend eine Weise *bestimmte* Zahlenwerthe sich vorzustellen; was hier *nicht* geschehen *soll.* Man mufs, um *nichts weiter* als den blofsen Begriff der *ganzen Zahl* zu bezeichnen, nothwendig einen Buchstaben nehmen, der nicht leicht auch noch in anderem Sinne gebraucht wird; und dann sogar festsetzen, dafs dieser Buchstabe *nie* zu irgend einer andern Bezeichnung gebraucht werden soll.

Zu diesem Zwecke scheint der deutsche Buchstab $\mathfrak{G}$, auch als der Anfangsbuchstab von „*Ganzes*" oder „*Ganze-Zahl*", passend. Einige französische Schriftsteller bedienen sich auf ähnliche Weise zur Bezeichnung des Begriffs der *ganzen Zahl* des Anfangsbuchstabs *E* des Wortes *entier.* Wir setzen daher fest:

Dafs der Buchstab $\mathfrak{G}$ ausschliefslich dazu dienen soll, eine ganze Zahl überall da zu bezeichnen, wo es auf die Gröfse der Zahl durchaus nicht ankommt.

VI. Wenn es also z. B. bei den Ausdrücken (2.), die zu der Untersuchung der Eigenschaften irgend einer Verbindung der ganzen Zahlen z_1, z_2, z_3, ... z_n mit einander und mit vielleicht noch anderen Zahlen in Beziehung auf die Zahl u dienten, auf die *Gröfse* der Quotienten q_1, q_2, q_3, ... q_n *nicht* ankäme, sondern nur darauf, dafs sie *ganze* Zahlen sind, so würde man statt der *verschiedenen* q in (2.) *gleichmäfsig* $\mathfrak{G}$ und folglich, statt wie in (2.), blofs

$$3. \begin{cases} z_1 = \mathfrak{G}u + r_1, \\ z_2 = \mathfrak{G}u + r_2, \\ z_3 = \mathfrak{G}u + r_3, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ z_n = \mathfrak{G}u + r_n \end{cases}$$

zu schreiben haben, wo nun ***einer und derselbe Buchstabe*** $\mathfrak{G}$ alle die verschiedenen Werthe von *q gleichzeitig* ausdrückt, oder wo vielmehr an die *Gröfse* der *ganzen* Zahlen, die $\mathfrak{G}$ bezeichnet, gar nicht mehr gedacht wird, sondern nur daran, *dafs* $\mathfrak{G}$ jedesmal eine *ganze* Zahl sein soll. Der Nutzen von Dergleichen wird sich in Dem was folgt zeigen.

VII. Diese Art des Gebrauchs eines Buchstabens, um Gröfsen oder Zahlen zu bezeichnen, ist zwar sonst nicht ganz gewöhnlich. Sie ist, wenn man will, etwas für die Theorie der Zahlen *Eigenthümliches.* Indessen ist einestheils das $\mathfrak{G}$ auch fast das *einzige* Eigenthümliche, was die Zahlentheorie in Anspruch nimmt, und fast alle übrigen Bezeichnungen und Operationen derselben sind ganz die nemlichen, wie in den übrigen Theilen des Calculs: anderntheils aber ist die Eigenthümlichkeit der Bezeichnungsart im Grunde doch *weniger* abweichend und vereinzelt, als sie es beim ersten Anblick zu sein scheint. Sie ist gewissermafsen nur eine Art von *Verallgemeinerung* des Gewöhnlichen; denn die Buchstaben überhaupt bezeichnen *gewöhnlich* schon *beliebige* Zahlen oder Gröfsen. Hier werden blofs noch die *Unterscheidungen* weggelassen, die man sonst zwischen den ***Buchstaben*** durch ihre Verschiedenheit oder durch Accente und dergleichen macht, weil die Unterscheidungen hier *nicht nöthig* sind.

VIII. Wenn nun in der Gleichung

$$4. \quad z = \mathfrak{G}u + r$$

$\mathfrak{G}$ in der angezeigten Bedeutung gebraucht wird, so nennt man eine solche Gleichung auch *Congruenz.*

Die beiden Zahlen z und r, deren Differenz $z - r$ oder $r - z$ durch *u theilbar* ist, indem (4.)

$$5. \quad z - r = \mathfrak{G}u \quad \text{und}$$

$$6. \quad r - z = -\mathfrak{G}u$$

giebt, für welches letztere man, da es auf die *Gröfse* von $\mathfrak{G}$ gar nicht ankommt, auch eben sowohl blofs

$$7. \quad r - z = \mathfrak{G}u$$

schreiben kann, und wo dann aus (5. u. 7.) hervorgeht, dafs $z - r$ und $r - z$

mit u *aufgehen*, weil $z-r$ und $r-z$ *Vielfache* von u, nemlich 𝔖fache sind, nennt man *zu einander congruent.*

Nicht congruent heifsen z und r, wenn $z-r$ oder $r-z$ *nicht* mit u aufgeht, also etwa

$$8.\quad z = \mathfrak{S}u + r + e$$

ist, wo e *nicht* mit u aufgeht, was

$$9.\quad z - r = \mathfrak{S}u + e \quad \text{und}$$

$$10.\quad r - z = \mathfrak{S}u - e$$

giebt und welches zeigt, dafs $z-r$ und $r-z$ *nicht* mit u aufgeht, indem solches der Voraussetzung nach mit e nicht der Fall ist.

Jede der beiden Zahlen z und r in (4.) nennt man *Residuum* der andern.

Den Divisor u nennt man auch *Modul*, und statt wie in (4.) schreibt man auch

$$11.\quad z \equiv r \pmod{u}.$$

Wir werden statt dieser letzten Art der Bezeichnung der Congruenzen die obige (4.) vermittels des 𝔖 beibehalten, weil dieselbe von Dem, was im übrigen Calcul gewöhnlich ist, weniger abweicht.

§. 11.

Lehrsatz.

Es bezeichne

$$1.\quad \mathrm{Z} = \mathrm{F}(\mathrm{z}_1, \mathrm{z}_2, \mathrm{z}_3, \ldots \mathrm{z}_n)$$

von den ganzen Zahlen $\mathrm{z}_1, \mathrm{z}_2, \mathrm{z}_3, \ldots \mathrm{z}_n$ *und von vielleicht noch andern ganzen Zahlen* $\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3, \ldots \mathrm{b}_1, \mathrm{b}_2, \mathrm{b}_3, \ldots$ *etc., welche dieselben bleiben, wenn die* z *ihre Werthe ändern, irgend eine Verbindung, welche folgende zwei Eigenschaften hat:*

Erstlich, dafs für alle möglichen ganzzahligen Werthe der z, *so wie der* a, *der* b *etc.,* Z *selbst ebenfalls immer eine ganze Zahl ist, und*

Zweitens, dafs wenn man nach (§. 10.)

$$2.\quad \begin{cases} \mathrm{z}_1 = \mathfrak{S}\mathrm{u} + \mathrm{r}_1, \\ \mathrm{z}_2 = \mathfrak{S}\mathrm{u} + \mathrm{r}_2, \\ \mathrm{z}_3 = \mathfrak{S}\mathrm{u} + \mathrm{r}_3, \\ \ldots \ldots \\ \mathrm{z}_n = \mathfrak{S}\mathrm{u} + \mathrm{r}_n \end{cases}$$

setzt, wo u, *und folglich die Reste* r, *ebenfalls lauter ganze Zahlen sind, darauf die Ausdrücke der* z (2.) *in* $\mathrm{F}(\mathrm{z}_1, \mathrm{z}_2, \mathrm{z}_3, \ldots \mathrm{z}_n)$ *substituirt und den daraus entstehenden Ausdruck von* Z *entwickelt, in diesem entwickel-*

ten Ausdrucke alle Glieder, in welchen u *vorkommt,* u *und ganze Zahlen zu Factoren haben und von den übrigen Gliedern, die* u *nicht enthalten, durch das Zeichen* + *oder* — *sich absondern lassen.*

Die sogenannten rationalen ganzen Functionen oder Verbindungen, nemlich diejenigen, in welchen von den Zahlen z, a, b, ... *nur Summen, Differenzen, Producte und Potenzen mit ganzzahligen positiven Exponenten vorkommen, nirgend Quotienten, Wurzelgröfsen, Exponentialgröfsen und andere transcendente Zahlen, haben jene beiden Eigenschaften; wie sich solches am besten an Beispielen zeigen wird.*

Für solche Verbindungen Z gilt nun im Allgemeinen Folgendes.

Wenn man nemlich in (1.) *statt der* z *ihre Ausdrücke* (2.) *setzt und den daraus entstehenden Ausdruck entwickelt, so hat derselbe immer die Form*

$$3.\quad Z = F(z_1, z_2, z_3, \dots z_n) = \mathfrak{G}u + F(r_1, r_2, r_3, \dots r_n);$$

das heifst, derjenige Theil $F(r_1, r_2, r_3, \dots r_n)$ *des entwickelten Ausdrucks von* Z, *in welchem kein* u *vorkommt, hat genau dieselbe Gestalt wie* Z *selbst, blofs dafs überall* r *statt* z *steht; so dafs man also diesen Theil unmittelbar erhält, wenn man in* (1.) *blofs überall* r *statt* z *schreibt.*

Beweis. Nach der *Voraussetzung* soll Z (1.), wenn man darin die Ausdrücke der verschiedenen z aus (2.) setzt, entwickelt, die Form

$$4.\quad Z = F(\mathfrak{G}u + r_1, \mathfrak{G}u + r_2, \mathfrak{G}u + r_3, \dots \mathfrak{G}u + r_n)$$
$$= u\varphi u + fr = \mathfrak{G}u + fr$$

haben, wo rechterhand der eine Theil $u\varphi u$ oder $\mathfrak{G}u$ des entwickelten Ausdrucks *durchweg u zum Factor hat*, der andere Theil fr *gar kein u* enthält.

Dieser Ausdruck gilt nun für alle möglichen ganzzahligen Werthe der z, und also auch für jeden ganzzahligen Werth von u; folglich auch für $u = 0$. Es ändert sich aber fr mit u *gar nicht*, weil es kein u enthält. Also bleibt in (4.) fr unverändert Dasselbe, auch wenn man $u = 0$ setzt, $u\varphi u$ hingegen verschwindet für $u = 0$, wegen des Factors u. Also giebt (4.), für $u = 0$:

$$5.\quad F(r_2, r_2, r_3, \dots r_n) = fr,$$

und folglich ist in (4.), wenn man darin fr aus (5.) substituirt und statt $u\varphi u$ blofs $\mathfrak{G}u$ schreibt, welches letztere angeht, da nach der Voraussetzung u und φu *ganze* Zahlen sein sollen,

$$6.\quad Z = F(z_1, z_2, z_3, \dots z_n) = \mathfrak{G}u + F(r_1, r_2, r_3, \dots r_n);$$

wie es der Lehrsatz in (3.) behauptet.

Beispiele. *No. 1.* Es sei

$$7.\quad Z = a_0 + a_1 z_1 + a_2 z_2 + a_3 z_3 \ldots + a_n z_n,$$

wo die a beliebige positive oder negative ganze Zahlen sind, die nicht von z abhängen.

Setzt man hierin die Ausdrücke der z aus (2.), so erhält man

$$Z = a_0 + a_1(\mathfrak{G}u + r_1) + a_2(\mathfrak{G}u + r_2) + a\,(\mathfrak{G}u + r_3) \ldots + a_n(\mathfrak{G}u + r_n) \text{ oder}$$
$$Z = u[a_1\mathfrak{G} + a_2\mathfrak{G} + a_3\mathfrak{G} \ldots + a_n\mathfrak{G}] + a_0 + a_1 r_1 + a_2 r_2 + a_3 r_3 \ldots + a_n r_n \text{ oder}$$
$$8.\quad Z = \mathfrak{G}u + a_0 + a_1 r_1 + a_2 r_2 + a_3 r_3 \ldots + a_n r_n;$$

denn was in a multiplicirt ist sind lauter ganze Zahlen.

Wie man sieht, besteht dieses Resultat aus zwei Theilen, deren einer die Form $\mathfrak{G}u$ hat, der andere unmittelbar aus Z (7.) hervorgeht, wenn man darin r statt z schreibt.

No. 2. Es sei

$$9.\quad Z = z_1 z_2,$$

so erhält man, wenn man die Ausdrücke (2.) der z substituirt:

$$10.\quad Z = (\mathfrak{G}u + r_1)(\mathfrak{G}u + r_2),$$

also, wenn man rechterhand die Factoren in einander multiplicirt,

$$Z = \mathfrak{G}\mathfrak{G}u^2 + \mathfrak{G}u.r_2 + \mathfrak{G}u.r_1 + r_1 r_2 \text{ oder}$$
$$Z = u[\mathfrak{G}\mathfrak{G}u + \mathfrak{G}r_2 + \mathfrak{G}r_1] + r_1 r_2 \text{ oder}$$
$$11.\quad Z = \mathfrak{G}u + r_1 r_2;$$

denn was in u multiplicirt ist, sind wieder lauter ganze Zahlen.

Das Resultat besteht wieder aus zwei Theilen, deren einer die Form $\mathfrak{G}u$ hat, der andere unmittelbar aus (9.) hervorgeht, wenn man r statt z schreibt.

No. 3. Es sei

$$12.\quad Z = z_1 z_2 z_3 \ldots z_m.$$

Für $Z = z_1 z_2$ war $Z = \mathfrak{G}u + r_1 r_2$ (11.), also ist für $Z = z_1 z_2 z_3$, $Z = (\mathfrak{G}u + r_1 r_2)(\mathfrak{G}u + r_3)$. Dieses giebt, wenn man multiplicirt, auf ganz ähnliche Weise wie in (10.), $Z = \mathfrak{G}u + r_1 r_2 r_3$. Daraus folgt weiter für $Z = z_1 z_2 z_3 z_4$, $Z = (\mathfrak{G}u + r_1 r_2 r_3)(\mathfrak{G}u + r_4)$, und wieder auf ähnliche Art wie in (10.), $Z = \mathfrak{G}u + r_1 r_2 r_3 r_4$, und so immer weiter bis

$$13.\quad Z = \mathfrak{G}u + r_1 r_2 r_3 \ldots r_m.$$

Auch hier ist der eine Theil des Resultats von der Form $\mathfrak{G}u$, der andere geht unmittelbar aus (12.) hervor, wenn man r statt z schreibt.

No. 4. Es sei

$$14.\quad Z = (a_0 + a_1 z_1 + a_2 z_2 \ldots + a_{n_1} z_{n_1}) \times (b_0 + b_1 z_1 + b_2 z_2 \ldots + b_{n_2} z_{n_2}) \times (c_0 + c_1 z_1 + c_2 z_2 \ldots + c_{n_3} z_{n_3}) \cdot \ldots \times (m_0 + m_1 z_1 + m_2 z_2 \ldots + m_{n_n} z_{n_n}).$$

Der Kürze wegen bezeichne man die Factoren rechterhand der Reihe nach durch $\varphi_1 z$, $\varphi_2 z$, $\varphi_3 z$, ... $\varphi_m z$, so dafs

$$15.\quad Z = \varphi_1 z \cdot \varphi_2 z \cdot \varphi_3 z \ldots \varphi_m z$$

ist. Setzt man hierin die Ausdrücke (2.) von z, so geht, da die Factoren φz ganz die Form von (7.) haben, zufolge (No. 1.)

$$16.\quad \varphi_1 z \text{ in } \mathfrak{S}u + \varphi_1 r, \quad \varphi_2 z \text{ in } \mathfrak{S}u + \varphi_2 r, \quad \varphi_3 z \text{ in } \mathfrak{S}u + \varphi_3 r \text{ u. s. w.}$$

über; also Z (15.) in

$$17.\quad Z = (\mathfrak{S}u + \varphi_1 r)(\mathfrak{S}u + \varphi_2 r)(\mathfrak{S}u + \varphi_3 r) \ldots (\mathfrak{S}u + \varphi_m r).$$

Man stelle sich vor, in (12. No. 3.) wären für die z, statt wie dort die Ausdrücke (2.), vielmehr der Reihe nach $z_1 = \mathfrak{S}u + \varphi_1 r$, $z_2 = \mathfrak{S}u + \varphi_2 r$, $z_3 = \mathfrak{S}u + \varphi_3 r$ u. s. w. gesetzt worden, so würden dort $\varphi_1 r$, $\varphi_2 r$, $\varphi_3 r$ etc. die Stellen von r_1, r_2, r_3 eingenommen haben. Also würde das Resultat, statt desjenigen (13.),

$$18.\quad Z = \mathfrak{S}u + \varphi_1 r \cdot \varphi_2 r \cdot \varphi_3 r \ldots \varphi_m r$$

gewesen sein. Dieses also ist das gegenwärtige zu (15.) oder (14.) gehörige Resultat. Auch dieses besteht aus einem Theil von der Form $\mathfrak{S}u$, und einem andern, der unmittelbar aus Z hervorgeht, wenn man darin r statt z schreibt.

No. 5. Es sei

$$19.\quad Z = z^m,$$

wo m irgend eine *ganze positive* Zahl ist.

Da diese Potenz z^m nichts anderes ist, als das Product von m Factoren, jeder gleich z, so erhält man was sich ergiebt, wenn man $\mathfrak{S}u + r$ statt z schreibt, unmittelbar aus (No. 3.), wenn man dort $z_1 = z_2 = z_3 \ldots = z_m = z$ und also auch $r_1 = r_2 = r_3 \ldots = r_m = r$ setzt. Das Resultat ist also

$$20.\quad Z = \mathfrak{S}u + r^m.$$

Dasselbe besteht wieder aus einem Theile von der Form $\mathfrak{S}u$, und einem andern, der unmittelbar aus (19.) sich ergiebt, wenn man r statt z setzt.

No. 6. Es sei

$$21.\quad Z = F(z_1, z_2, z_3, \ldots z_m) = z_1^{m_1} \cdot z_2^{m_2} \cdot z_3^{m_3} \ldots z_n^{m_n}.$$

Setzt man hierin die Ausdrücke der z aus (2), so geht zufolge (No. 5.) Z in

$$22.\quad Z = (\mathfrak{G}u + r_1^{m_1})(\mathfrak{G}u + r_2^{m_2})(\mathfrak{G}u + r_3^{m_3}) \ldots (\mathfrak{G}u + r_n^{m_n})$$

über; und ganz auf ähnliche Weise wie in (No. 3.) findet sich, dafs das Product rechterhand, und folglich Z, nichts anderes ist als

$$23.\quad Z = \mathfrak{G}u + r_1^{m_1}.r_2^{m_2}.r_3^{m_3} \ldots r_n^{m_n}.$$

Das Resultat ist, wie man sieht, wieder von der Form $\mathfrak{G}u + Fr$.

Ähnliches wird man immer finden, wenn auch Z eine noch mehr zusammengesetzte *ganze rationale* Verbindung ist; z. B. wenn in (14.) an der Stelle der verschiedenen z Producte verschiedener Potenzen der z wie (21.) stehen, u. s. w.

Anm. Zu bemerken ist, dafs der Lehrsatz durchaus *nur dann* unbedingt gilt, wenn die obigen *beiden Bedingungen* für Z erfüllt werden, und also nur für *ganze rationale* Verbindungen. Schon z. B. für

$$24.\quad Z = \frac{a+z}{b+z} = Fz$$

ist, wenn man $z = \mathfrak{G}u + r$ setzt, nicht nothwendig

$$25.\quad Z = \mathfrak{G}u + \frac{a+r}{b+r} = \mathfrak{G}u + Fr,$$

das heifst

$$26.\quad \frac{a+z}{b+z} - \frac{a+r}{b+r} = \mathfrak{G}u;$$

denn es folgt keinesweges, dafs der *Bruch* $\frac{a+z}{b+z}$ von dem Bruch $\frac{a+r}{b+r}$ für *jeden beliebigen* Werth von z und r um eine *ganze* Zahl, geschweige denn grade um ein Vielfaches $\mathfrak{G}u$ von u verschieden sei.

Anm. Der Rest $F(r_1, r_2, r_3, \ldots r_n)$ (3.) von $Z = F(z_1, z_2, z_3, \ldots z_n)$ zu dem Quotienten u ist übrigens nicht nothwendig ein *echter* Rest von Z zu u; selbst dann nicht, wenn die r in (2.) sämmtlich *echte* Reste zu den z sind; denn $F(r_1, r_2, r_3, \ldots r_n)$ kann *viel gröfser* sein als u. Auch ist es, wenn man einen echten Rest zu Z haben will, keineswegs nöthig, erst $F(r_1, r_2, r_3, \ldots r_n)$ wirklich zu berechnen, sondern man kann dazu in den einzelnen Fällen vermittels *kleinerer* Zahlen gelangen.

Anstatt nemlich z. B. in (8.) den Rest $a_0 + a_1 r_1 + a_2 r_2 \ldots + a_n r_n$ ganz zu berechnen, nehme man erst die *echten* Reste zu a_0 und $a_1 r_1$ und ihre *Summe*. Ist diese Summe gröfser als u, so nehme man von ihr wieder erst den *echten* Rest, thue ihn zu demjenigen von $a_2 r_2$, verfahre mit der Summe wie vorhin, thue den echten Rest von $a_3 r_3$ hinzu, u. s. w. bis zu Ende. Dadurch werden

beständig noch *Vielfache von* u abgesondert, die zu $\mathfrak{G}u$ geschlagen werden können, und man gelangt zu dem *echten Rest* von Z vermittels *kleinerer* Zahlen.

Anstatt in (12.) das Product $r_1, r_2, r_3, \ldots r_m$ zu berechnen und davon den echten Rest nach u zu nehmen, berechne man erst den *echten* Rest zu $r_1 r_2$, multiplicire ihn mit r_3, nehme von dem Product den *echten* Rest, multiplicire diesen mit r_4, nehme wieder von dem Product den *echten* Rest, u. s. w. bis zu Ende, so gelangt man zu dem *echten* Rest von $Z = z_1, z_2, z_3, \ldots z_m$ wieder vermittels *kleinerer* Zahlen.

Wäre z. B. der *echte positive* Rest des Products

$$27.\quad Z = 18.25.41.64.123.191$$

zu der Zahl 13 zu berechnen, so ist nach (2.)

$$28.\quad \begin{cases} 18 = \mathfrak{G}.13 + 5, \\ 25 = \mathfrak{G}.13 + 12, \\ 41 = \mathfrak{G}.13 + 2, \\ 64 = \mathfrak{G}.13 + 12, \\ 123 = \mathfrak{G}.13 + 6, \\ 191 = \mathfrak{G}.13 + 9, \end{cases}$$

und nach (13.)

$$29.\quad Z = \mathfrak{G}.13 + 5.12.2.12.6.9.$$

Aber das Product 5.12.2.12.6.9 ist keineswegs der echte positive Rest von Z zu $u = 13$, obgleich alle r in (28.) *positive echte* Reste zu den z sind. Um den echten positiven Rest zu Z zu finden, nehme man erst $r_1 r_2 = 5.12 = \mathfrak{G}.13 + 8$, multiplicire dies mit $r_3 = 2$, welches $r_1 r_2 r_3 = 2(\mathfrak{G}.13+8) = \mathfrak{G}.13 + 16 = \mathfrak{G}.13 + 13 + 3 = \mathfrak{G}13 + 3$ giebt. Dieses multiplicire man mit $r_4 = 12$, so erhält man $r_1 r_2 r_3 r_4 = 12(\mathfrak{G}.13+3) = \mathfrak{G}13 + 36 = \mathfrak{G}13 + 2.13 + 10 = \mathfrak{G}.13 + 10$. Dieses multiplicire man mit $r_5 = 6$, so ergiebt sich $r_1 r_2 r_3 r_4 r_5 = 6(\mathfrak{G}.13+10) = \mathfrak{G}13 + 60 = \mathfrak{G}13 + 4.13 + 8 = \mathfrak{G}13 + 8$. Dieses endlich mit $r_6 = 9$ multiplicirt, giebt $9(\mathfrak{G}13+8) = \mathfrak{G}13 + 72 = \mathfrak{G}13 + 5.13 + 7 = \mathfrak{G}13 + 7$. Also ist

$$30.\quad r_1 r_2 r_2 r_3 r_4 r_5 r_6 = \mathfrak{G}13 + 7$$

und vermöge (29.)

$$31.\quad Z = \mathfrak{G}.13 + \mathfrak{G}13 + 7 = \mathfrak{G}13 + 7,$$

und folglich ist 7 der *echte positive* Rest von Z (27.) zu $u = 13$.

Verlangt man den *unbedingt echten* Rest von Z (27.), so kann man auch sogleich die *unbedingt echten* Reste der Factoren z nehmen; welches *noch kleinere* Zahlen giebt. Es ist nemlich z. B. alsdann statt (28.)

$$32. \quad \begin{cases} 18 = \mathfrak{G}.13+5, \\ 25 = \mathfrak{G}.13-1, \\ 41 = \mathfrak{G}.13+2, \\ 64 = \mathfrak{G}.13-1, \\ 123 = \mathfrak{G}.13+6, \\ 191 = \mathfrak{G}.13-4. \end{cases}$$

Hier ist $r_1 r_2 = \mathfrak{G}13 - 5.1 = \mathfrak{G}13 - 5$. Dieses, mit $r_3 = 2$ multiplicirt, giebt $r_1 r_2 r_3 = 2(\mathfrak{G}13 - 5) = \mathfrak{G}13 - 10 = \mathfrak{G}13 + 3$. Dieses, mit $r_4 = -1$ multiplicirt, giebt $r_1 r_2 r_3 r_4 = -1(\mathfrak{G}13 + 3) = \mathfrak{G}13 - 3$. Dies, mit $r_5 = 6$ multiplicirt, giebt $r_1 r_2 r_3 r_4 r_5 = 6(\mathfrak{G}13 - 3) = \mathfrak{G}13 - 18 = \mathfrak{G}13 - 5$, und dieses, mit $r_6 = -4$ multiplicirt, giebt $-4(\mathfrak{G}13 - 5) = \mathfrak{G}13 + 20 = \mathfrak{G}13 - 6$; so dafs der ***unbedingt echte*** Rest von Z (27.) zu u, -6 ist.

§. 12.

Erklärungen und Erläuterungen.

I. Ganze Zahlen, die mit keiner andern ganzen Zahl > 1 als mit sich selbst aufgehen, wie z. B. die Zahlen 2, 3, 5, 7, ... 53, 157, ... 353 u. s. w. kann man ***Stammzahlen*** nennen, weil die übrigen aus ihnen durch Multiplication zusammengesetzt werden können, und also von ihnen ***abstammen***. Gewöhnlich heifsen sie ***Primzahlen***. Noch besser, als eine ***bildliche*** deutsche oder fremde Benennung, wäre die geradezu ***bezeichnende*** Benennung ***theilerlose*** oder ***untheilbare Zahlen***. Doch ist ***Stammzahl*** kürzer.

II. Ganze Zahlen, welche, aufser mit sich selbst, auch noch mit andern ganzen Zahlen > 1 aufgehen, wie z. B. 15, was mit 3 und 5; 84, was mit 2, 3, 4, 6, 7, 12, 14, 21, 28 und 42 aufgeht u. s. w., nennt man gewöhnlich ***zusammengesetzte Zahlen***. Kürzer und bezeichnender ist ***theilbare Zahlen***. Zwar liefse sich dagegen sagen, dafs Zahlen auch noch auf andere Weise als durch Division theilbar sind, nemlich durch Subtraction; was auch selbst bei den Stammzahlen der Fall ist. Aber der Einwand trifft auch eben sowohl die Benennung ***zusammengesetzte*** Zahl; denn nicht blofs durch Multiplication, sondern auch durch Addition können Zahlen aus andern ***zusammengesetzt*** werden. ***Theilbare Zahl*** aber ist ***kürzer***, und dürfte also besser sein. Man darf nur das Wort ***theilen*** ausschliefslich der ***Division*** vorbehalten und statt Theilen durch Subtraction ***zerlegen*** setzen, so ist die Benennung ***theilbare Zahl*** vollständig und ausschliefslich ***bezeichnend***.

III. Zwei ganze Zahlen, welche mit keiner ganzen Zahl >1 *beide zugleich* aufgehen, und die also einander rücksichtlich ihrer Theilbarkeit oder ihrer Theiler *fremd* sind, wie z. B. 8 und 15, 165 und 238 u. s. w., nennt man gewöhnlich *relative Primzahlen.* Natürlicher wäre es, sie geradezu, nach ihrer vorhin bezeichneten Eigenschaft, *theilerfremde Zahlen* zu nennen. Alle Stammzahlen sind einander *theilerfremd.*

IV. Zweien oder mehreren Zahlen, welche mit andern ganzen Zahlen >1 *zugleich* aufgehen, z. B. 105 und 154, die mit 7; 66 und 102, die mit 2, 3 und 6; 30, 105 und 195, die mit 3, 5 und 15 aufgehen u. s. w. pflegt man gewöhnlich nicht eigentlich eine besondere Benennung beizulegen. Natürlich wäre es indessen, solche Zahlen, im Gegensatz zu den *theilerfremden* Zahlen, *theilerverwandte* Zahlen zu nennen. Die Beiwörter *theilerverwandt* und *theilerfremd* dürften andern, ganz gebräuchlichen, zu ähnlichen Zwecken zusammengesetzten Beiwörtern, z. B. den Beiwörtern *sinnverwandt* und *sinnfremd,* als nachgebildet zu betrachten und also *grammatisch* nicht zu verwerfen sein.

V. Diejenigen ganzen Zahlen >1, welche in zwei oder mehrere ganze Zahlen *zugleich* aufgehen, nennt man ihre *gemeinschaftlichen* Theiler und die gröfste unter ihnen *gröfsten gemeinschaftlichen Theiler.* Kürzer wäre *Gemeintheiler* und *gröfster Gemeintheiler;* nach dem Vorbilde z. B. des Wortes *Gemeingut.*

VI. Für mehr als *zwei* Zahlen reicht die Benennung *theilerfremd* nicht aus, um alles was nöthig ist auszudrücken; die Benennung *relative Primzahl* ebenso wenig. Denn es können Zahlen, wenn ihrer mehr als zwei sind, ohne *gemeinschaftliche* Theiler sein, während sie gleichwohl *nicht* relative Primzahlen sind. Zum Beispiel die 6 Zahlen $198 = 2.3^2.11$, $165 = 3.5.11$, $255 = 3.5.17$, $154 = 2.7.11$, $228 = 2^2.3.19$ und $715 = 5.11.13$ haben *keinen gemeinschaftlichen* Theiler: gleichwohl ist *keine* zu der andern relative Primzahl, sondern 198 hat mit 165, 255 und 228 den Theiler 3, mit 154 und 228 den Theiler 2, mit 165, 154 und 715 den Theiler 11 gemein u. s. w. Man kann also solche Zahlen weder theilerfremd noch relative Primzahlen nennen. Die Benennung für sie ergiebt sich aber aus (V.) von selbst. Sie haben nemlich keinen *Gemeintheiler* und müssen folglich *gemeintheilerfremd* heifsen. *Zwei* Zahlen, wenn sie theilerfremd sind, sind auch gemeintheilerfremd, und daher genügt für *zwei* Zahlen die Benennung *theilerfremd.*

Mehr als zwei Zahlen dagegen können gleichzeitig *gemeintheilerfremd* und *theilerverwandt* sein.

VII. Haben mehr als zwei Zahlen *Gemeintheiler*, wie z. B. 198, 165, 255 und 228, die alle mit 3 aufgehen, so werden sie *gemeintheilerverwandt* heifsen müssen. Dergleichen Zahlen sind natürlich auch immer *theilerverwandt*. Für blofs zwei Zahlen genügt *theilerverwandt*; denn sind sie das, so sind sie auch *gemeintheilerverwandt*.

VIII. Zwei ganze Zahlen, deren Summe oder Differenz mit einer bestimmten dritten ganzen Zahl aufgeht, wie z. B. die Zahlen z und r in der Gleichung $z = \mathfrak{G}u \pm r$, deren Summe oder Differenz $z \pm r$ mit der Zahl u aufgeht, und die man gewöhnlich nach (§. 10. VIII.) *zu einander nach dem Modul u congruent* nennt, könnte man deutsch *zu einander nach dem Theiler u theilbar* nennen. Das Wort *zu* würde das Zueinanderhinzuthun der beiden Zahlen andeuten.

IX. Je nachdem Zähler und Nenner eines Bruches *theilerfremd* oder *theilerverwandt* sind, nennt man gewöhnlich den Bruch *irreducibel* oder *reducibel*, und das Wegschaffen der Gemeintheiler von Zähler und Nenner *Reduciren* des Bruchs. Gegenbildlich zu den allgemein gebräuchlichen Benennungen *echter* und *unechter* Bruch, könnte man irreducible Brüche *reine*, reducible *unreine* nennen. Statt *reduciren* könnte es heifsen: einen Bruch *aufheben* oder, wenn man will, *reinigen*.

X. Sind die ganzzahligen Factoren einer Zahl untheilbar oder Stammzahlen, so heifsen sie folgerichtig *Stammfactoren*.

Besser als bildliche oder willkürliche Benennungen sind unstreitig überall, und folglich auch, und sogar ganz besonders in der *Mathematik*, solche Benennungen, die ihren Gegenstand möglichst gradezu bezeichnen; denn sie begünstigen weniger die Verwechselungen. Es ist zweifelsohne überall gut, die Dinge bei ihrem rechten Namen zu nennen.

Sodann sind wohl unstreitig Benennungen aus der Sprache selbst, in welcher man sich ausdrückt, schon im Allgemeinen besser, als Benennungen aus andern Sprachen; denn sie verstärken die Deutlichkeit und Verständlichkeit der Rede. Sind die Benennungen aus der eigenen Sprache *eben so* bezeichnend, oder bezeichnender als die fremden, so ist es gradezu *unrecht*, die letztern statt jener zu setzen; denn es kann dann nur aus *Verachtung* der

eigenen Sprache geschehen; und zu dieser haben die Deutschen wohl ebenso wenig, wie irgend ein anderes Volk, Ursach.

Es ist zwar nicht unwahrscheinlich, dafs *alle* fremden Benennungen, auch in der Mathematik, durch deutsche sich ersetzen lassen; und wären selbst nur *bildliche* Benennungen zu finden, so wären sie, als spracheigen, gleichwohl noch besser, als die fremden, insofern diese ebenfalls, wie z. B. die fremden Wörter Product, Factor, Sinus, Cosinus, positiv, negativ, rational, irrational, Factorielle, Facultät, Differential, Integral u. s. w., nur bildlich sind. Indessen ist es gewifs gut, die Verdeutschung *solcher* Ausdrücke mehr der Zeit zu überlassen, weil das, was nicht zugleich *in sich* entschieden besser ist, als das Fremde, durch seine Heimathlichkeit allein vielleicht nicht Recht genug hat, das in Besitz begriffene Fremde zu vertreiben. Wo dagegen völlig *bezeichnende* deutsche Benennungen ganz bereit zur Hand sind, haben sie *volles Recht,* die Stelle der fremden einzunehmen.

Dafs übrigens etwa die Einführung weniger oder gar noch nicht gewöhnlicher Benennungen das Studium einer Wissenschaft erschweren werde, ist nicht zu fürchten, sobald nur die neuen Worte ihre Gegenstände mehr beim rechten Namen nennen, als die alten, oder auch nur für ähnliche Begriffe schon gäng und gebe sind. Das Ungewohnte darf nur allein dann zurückgewiesen werden, wenn es in sich *weniger gut* ist, als das Gewohnte; *niemals* wenn es *besser* ist.

In diesen Erwägungen liegen die Gründe zu den Aufstellungen des gegenwärtigen Paragraphs. Die Absicht, deutsche Worte, welche bezeichnender sein mögen, als die gewöhnlichen fremden, für einige Gegenstände der vorliegenden Abhandlung statt der fremden zu setzen, ist übrigens auch den Erfolgen, die die Erfahrung längst ergeben hat, nicht entgegen. Auch in der Mathematik sind in der neuern Zeit schon statt *vieler* fremden Worte deutsche ziemlich allgemein angenommen worden; z. B. Unterschied statt Differenz, Vielfaches statt Multiplum, Verhältnifs statt Proportion, Reihe statt Progression, Dreieck, Viereck, Vieleck, Kegel, Kugel, statt Triangel, Quadrangel, Polygon, Conus, Sphaere u. s. w. Es ist also hier in diesem Paragraph nur etwas geschehen, was dem *erfahrungsmäfsig* wirklich stattfindenden Bestreben *gemäfs* ist; nichts, was ihm *entgegen* wäre. Daher werden wir uns der hier aufgestellten Benennungen in Dem was folgt statt der sonst gewöhnlichen bedienen.

§. 13.

Erläuterung.

A. Eine *ganze Zahl* drückt die Gröfse der *Menge* von einzelnen Dingen aus, welche man, indem man sie zusammenfafst, in irgend einer Beziehung als unter einander *gleich* betrachtet. Die Zahl für ein einzelnes Ding ist die *Einheit. Ziffern* sind die Zeichen für ganze Zahlen, wenn die Gröfse der Mengen *bestimmt* ist; *Buchstaben,* oder beliebige andere Zeichen sind es, wenn die Gröfse der Mengen *unbestimmt* ist.

B. Für den Begriff der Gröfse der Menge an sich, oder der Zahl, ist es offenbar völlig gleichgültig, *welche* Dinge es sind, deren Menge die Zahl vorstellt. In diesem Sinne ist es *nicht* angemessen, eine Zahl, *ohne* Rücksicht auf die Dinge welche sie *zählt, unbenannte* Zahl, und dagegen die Gesammtheit der Dinge *selbst,* welche die Zahl zusammenfafst, *benannte Zahl* zu nennen. Die Dinge *selbst* können niemals eine *Zahl* sein; es kann immer nur heifsen: eine Zahl *benannter Dinge.* Der Begriff der Zahl ist abstract, oder von den Dingen, auf welche er angewendet wird, *abgezogen.* Er liegt nicht *in* den Dingen, sondern wird auf sie *angewendet.*

C. Es können aber nicht blofs Dinge, die in irgend einer Beziehung als unter einander gleich betrachtet werden, zu zählen sein, sondern es können auch Dinge, wenn sie beliebig *theilbar* sind, in *Theile* zu *theilen* sein, die ihrerseits unter sich in irgend einer Beziehung als gleich betrachtet werden. Es ist also zunächst auch noch auszudrücken nöthig, in *wieviele* gleiche Theile etwa ein Ding, welches als Einheit betrachtet wird, zu theilen sei; und dann, wieviele *solcher Theile* genommen werden sollen. Da es hier wiederum nur auf die Gröfse von *Mengen* ankommt, nemlich erstlich auf die *Menge* der *gleichen Theile,* welche *ein einzelnes Ding ausmachen* sollen, und dann zweitens auf die *Menge* dieser *Theile,* welche zu nehmen sind, so kann beides ebenfalls durch die *Zahl* geschehen. Wie man die Zahlen, welche hier das Verlangte anzeigen, zu einander stellen will, ist *willkürlich.* Man schreibt, wenn z. B. ein Ding in *b* gleiche Theile zu theilen ist und *a* solcher Theile genommen werden sollen, wo dann *a* und *b* Zeichen *ganzer* Zahlen sind,

1. $\frac{a}{b}$ oder auch $a:b$,

und nennt diesen Zahlen-Ausdruck *Bruch, a* den *Zähler, b* den *Nenner* des Bruchs.

D. Brüche und ganze Zahlen reichen für *alle* Fälle, welche in der Rechnung vorkommen können, *vollständig* aus; denn auch Irrationales, so wie Transcendentes, sind nur *Grenzen* gewisser nach diesem oder jenem Gesetz sich richtender *Brüche;* und selbst Imaginäres geht nur erst aus der Rechnung mit Zahlen hervor.

Da nun Brüche eben sowohl *Mengen zählen,* als ganze Zahlen, nemlich *Theile* von Dingen, die als neue Einheiten betrachtet werden, so kann man füglich die Bedeutung des Worts *Zahl verallgemeinern,* und es eben sowohl ganze Zahlen, als Brüche ausdrücken lassen. Mengen von *Einheiten* heifsen dann *ganze Zahlen,* Mengen von *Theilen* von Einheiten *Brüche;* beide gleichmäfsig *Zahlen.* Darstellbar sind Brüche durch ganze Zahlen immer.

E. Da $\frac{a}{b}$ nach (*C.*) a gleiche Theile bezeichnet, deren b die Einheit ausmachen, so drückt $\frac{1}{b}$ *einen* dieser Theile aus: denn für *einen* solchen Theil ist der *Zähler* a der Theile gleich 1. Also bezeichnet $a.\frac{1}{b}$ *dasselbe,* wie $\frac{a}{b}$, und folglich ist

$$2. \quad \frac{a}{b} = a.\frac{1}{b}.$$

F. Auch kommt offenbar Dasselbe heraus, ob man die Einheit in b Theile theilt und a solcher Theile nimmt, oder ob man a Einheiten als ein *Ganzes* betrachtet und dieses Ganze in b Theile theilt: denn, so wie *a Einheiten* das Ganze a zusammensetzen, so setzen auch, *nach der Theilung* des Ganzen a in b Theile, a einzelne *Theile* der Einheit, jeder $= \frac{1}{b}$, den bten Theil $\frac{a}{b}$ des Ganzen a zusammen. Also kann man sich $\frac{a}{b}$ statt als a bte Theile der Einheit, auch als den bten Theil des Ganzen a vorstellen.

G. Wenn $\frac{a}{b}$ mit der ganzen Zahl c zu *multipliciren* ist, was durch $c.\frac{a}{b}$ auszudrücken sein wird, so folgt zunächst aus (2.)

$$3. \quad c.\frac{a}{b} = c.a.\frac{1}{b},$$

das heifst, rechterhand: a Dinge oder Einheiten, jedes $= \frac{1}{b}$, sind cmal zu nehmen. Aber die ganze Zahl ca drückt eben soviel Einheiten aus als c*mal* a. Dieses ist kein zu *beweisender* sondern ein willkürlicher Satz. Erst dafs $ca = ac$ sei, oder dafs amal c eben soviele Einheiten enthält, als cmal a,

ist ein des Beweises bedürfender Satz. Es ist derjenige (§. 6.), und er ist dort bewiesen.

Also kann statt (3.) auch geschrieben werden:

$$4. \quad c.\frac{a}{b} = ca.\frac{1}{b}.$$

Aber eben so wie $\frac{1}{b}$, mit der ganzen Zahl a multiplicirt, soviel ist als $\frac{a}{b}$ (2.), ist auch $\frac{1}{b}$ mit der ganzen Zahl ca multiplicirt soviel als $\frac{ca}{b}$. Also ist

$$5. \quad ca.\frac{1}{b} = \frac{ca}{b} = c.\frac{a}{b}.$$

H. Wenn der *b*te Theil der Einheit weiter in *c* gleiche Theile getheilt wird, so machen *c* solcher Theile $\frac{1}{b}$ aus. Nimmt man also statt *c* jener Theile, ihrer *bmal c*, so hat man das *b*fache des Resultats $\frac{1}{b}$. Dieses aber ist $= 1$. Also machen *b*mal *c*, oder, was dasselbe ist, *bc* jener *c*ten vom *b*ten Theile der Einheit die Einheit aus. Eben das ist mit dem *bc*ten Theile der Einheit der Fall, also ist

$$6. \quad \frac{1}{b} : c = \frac{1}{bc}.$$

Auch ist demnach

$$7. \quad \frac{a}{b} : c = \frac{a}{bc};$$

denn $\frac{a}{b}$ ist $= a.\frac{1}{b}$ (2.), also $\frac{a}{b} : c = a.\frac{1}{b} : c = a.\frac{1}{bc}$ (6.) $= \frac{a}{bc}$ (2.).

I. Wenn $\frac{a}{bc}$ mit *c* zu multipliciren ist, welches durch $c.\frac{a}{bc}$ auszudrücken sein wird, so ist erstlich wegen $\frac{a}{bc} = a.\frac{1}{bc}$ (2.), $c.\frac{a}{bc} = c.a.\frac{1}{bc}$ $= a.c.\frac{1}{bc}$. Aber $\frac{1}{bc}$ kann man sich nach (6.) als $\frac{1}{b}$ *dividirt* durch *c* vorstellen. Da nun hier $\frac{1}{bc}$ oder $\frac{1}{b}$, *dividirt* durch *c*, wieder zunächst *cmal zu nehmen* ist, so giebt $c.\frac{1}{bc} = \frac{1}{b}$. Also ist $a.c.\frac{1}{bc} = a.\frac{1}{b}$ und dieses ist $= \frac{a}{b}$ (2.). Aber es ist $a.c.\frac{1}{bc} = ac.\frac{1}{bc} = \frac{ac}{bc}$ (2.): also ist

$$8. \quad \frac{ac}{bc} = \frac{a}{b};$$

das heifst: *gleiche* Factoren im Zähler und Nenner eines Bruchs *heben sich auf.* Diese nähere Erörterung wegen des *Aufhebens* der Factoren in Brüchen war des Folgenden wegen nöthig.

§. 14.

Lehrsatz.

I. *Jede ganze Zahl geht nothwendig mit jedem ihrer ganzzahligen Factoren auf, das heifst: wenn man die Zahl durch den Factor dividirt, so ist der Quotient eine ganze Zahl; oder auch, wenn man den Factor wiederholt von der Zahl abzieht, so bleibt zuletzt Null.*

II. *Jede ganze Zahl, die in eine andere ganze Zahl aufgeht, ist einer ihrer Factoren.*

III. *Wenn der Quotient, z. B. der ganzen Zahl* z, *dividirt durch die ganze Zahl* u, *eine ganze Zahl* w *ist, so geht* u *in* z *nothwendig auf.*

Beweis von I. Es seien u_1, u_2, u_3, ... u_n die verschiedenen ganzzahligen Factoren der ganzen Zahl z, so dafs

$$1. \quad z = u_1 . u_2 . u_3 \ldots . u_n$$

ist. Da die u sämmtlich ganze Zahlen sind, so ist z. B. auch $u_2 . u_3 \ldots . u_n$ eine ganze Zahl, folglich ist, wenn man dieselbe durch v bezeichnet

$$2. \quad z = u_1 . v.$$

Aus (2.) folgt, dafs der Factor u_1 vmal in z enthalten ist, also, vmal davon abgezogen, der Rest Null bleibt, oder dafs u_1 in z aufgeht. Gleiches gilt von jedem andern Factor von z.

Beweis von II. Wenn u_1 in z aufgeht, oder, z. B. vmal von z abgezogen, Null läfst, so ist z aus vmal u_1 zusammengesetzt, und folglich u_1 ein Factor von z.

Beweis von III. Wenn man

$$3. \quad \frac{z}{u} = w$$

setzt, so ist nach (§. 13. 5. *I.*)

$$4. \quad u . \frac{z}{u} \text{ oder } u . w = \frac{u . z}{u} = z.$$

Wenn also nun w eine *ganze* Zahl ist, so folgt aus (4.), dafs u eine ganze Zahl von Malen in z enthalten ist, also in z aufgeht.

§. 15.

Lehrsatz.

I. *Wenn irgend ein Factor* v_1 *einer ganzen Zahl*

$$1. \quad u = v_1 . v_2 . v_3 . \ldots . v_n$$

in eine ganze Zahl z *nicht aufgeht, so geht auch* u *selbst nicht in* z *auf.*

II. *Wenn* u *in* z *aufgeht, so geht auch jeder Factor* v *von* u *in* z *auf.*

Beispiel zu I. Der Factor 3 der Zahl $u = 78 = 2.3.13$ geht in die Zahl $z = 1430 = 2.5.11.13$ *nicht* auf; und auch $u = 78$ geht in 1430 nicht auf, obgleich die übrigen Factoren 2, 13 und 26 in 1430 aufgehen.

Beispiel zu II. Die Zahl $u = 286 = 2.11.13$ geht in $z = 1430 = 2.5.11.13$ auf. Und auch alle die Factoren 2, 11, 13, 22, 26 und 143 von 286 gehen in 1430 auf.

Beweis von I. Man setze

$$2.\quad v_2.v_3.v_4 \ldots . v_n = y,$$

so dafs in (1.)

$$3.\quad u = v_1.y \quad \text{und} \quad y = \frac{u}{v_1} \quad (\text{§. 14. I.})$$

ist. Ferner sei

$$4.\quad \frac{z}{v_1} = w_1 \quad \text{und}$$

$$5.\quad \frac{z}{u} \quad \text{oder} \quad \frac{z}{v_1 . y} \ (3.) = w.$$

Man multiplicire (5.) mit y, so erhält man

$$6.\quad wy = y.\frac{z}{v_1 y} = \frac{yz}{v_1 y} = \frac{z}{v_1} \quad (\text{§. 13. } \mathit{I}.).$$

Daher ist, (6.) in (4.) gesetzt,

$$7.\quad w_1 = wy.$$

Nun geht nach der Voraussetzung v_1 in z *nicht* auf. Also ist zufolge (4.) w_1 *nicht* eine ganze Zahl. Gingen dagegen u in z auf, so wäre nach (5.) w eine *ganze* Zahl. Aber auch y (2.) ist eine ganze Zahl, und folglich auch wy, welches nach (7.) *gleich* w_1 sein soll. Also wäre eine ganze Zahl einer nicht ganzen Zahl gleich. Aus diesem Widerspruch folgt, dafs, wenn irgend ein Factor v_1 von u in z *nicht* aufgeht, auch u selbst nicht in z aufgehen kann.

Beweis von II. Wenn u in z aufgeht, so ist w (5.) eine ganze Zahl; desgleichen ist, wenn v_1 irgend einen Factor von u bezeichnet, y in (3.) eine ganze Zahl. Nun ist nach (§. 13. *I.*)

$$8.\quad u.\frac{z}{u} \quad \text{oder} \quad u.w = \frac{uz}{u} = z \quad \text{und}$$

$$9.\quad v.\frac{u}{v_1} \quad \text{oder} \quad v_1 . y \ (3.) = \frac{v_1 u}{v_1} = u:$$

also, wenn man (9.) in (8.) setzt,

$$10. \quad z = v_1 y w.$$

Da nun nach der Voraussetzung w und y ganze Zahlen sind, so ist auch yw eine ganze Zahl, und folglich ist der Factor v_1 von u eine ganze Zahl yw von Malen in z enthalten, und geht folglich in z auf. Gleiches gilt von jedem andern Factor von u. Also geht jeder Factor von u in z auf, wenn u selbst in z aufgeht.

§. 16.

Lehrsatz.

Wenn eine ganze Zahl z *mit einer andern ganzen Zahl* u *aufgeht, so ist der Quotient der Division der nemliche, man mag* z *auf einmal mit* u *dividiren, oder erst durch irgend einen der Factoren* v_1 *von* u, *darauf den Quotienten dieser Division durch irgend einen andern Factor* v_2 *von* u, *den Quotienten hievon durch einen dritten Factor* v_3 *von* u *u. s. w. Nur mufs die zweite Art der Division so lange fortgesetzt werden, bis alle Factoren* v *von* u *erschöpft sind. Alle bei dieser zweiten Art der Division sich ergebenden Quotienten sind der Reihe nach ganze Zahlen. Die Ordnung, in welcher man bei dem zweiten Verfahren die Factoren* v *von* u *zu Divisoren nimmt, ist willkürlich. Auch bleibt der Satz unverändert derselbe, wenn die Factoren* v *von* u, *alle oder einige, unter einander gleich sind.*

Beispiel. $z = 84$, durch $u = 12 = 2.2.3$ auf einmal dividirt, giebt 7. Andrerseits ist

$$1. \quad \begin{cases} \frac{84}{2} = 42, & \frac{42}{2} = 21, \quad \frac{21}{3} = 7, \\ \frac{84}{3} = 28, & \frac{28}{4} = 7, \\ \frac{84}{6} = 14, & \frac{14}{2} = 7, \\ \frac{84}{4} = 21, & \frac{21}{3} = 7, \\ \frac{84}{2} = 42, & \frac{42}{6} = 7 \quad \text{u. s. w.} \end{cases}$$

Immer ist der letzte Quotient der nemliche, und alle darauf führenden Quotienten sind *ganze* Zahlen.

Beweis. *A.* Da *nach der Voraussetzung* z mit

$$2. \quad u = v_1 . v_2 . v_3 \ldots . v_n,$$

wo die v beliebige theilbare oder untheilbare Factoren von u sein können, aufgehen soll, so geht zufolge (§. 15. II.) z auch mit *jedem* dieser Factoren v von u auf.

B. Nun sind v_1, $v_1 v_2$, $v_1 v_2 v_3$, ... sämmtlich Factoren von ***u***, also sind, wenn man

$$3.\quad \frac{z}{v_1} = w_1,\quad \frac{z}{v_1 v_2} = w_2,\quad \frac{z}{v_1 v_2 v_3} = w_3,\ \ldots\ \frac{z}{v_1 v_2 v_3 \ldots v_{k-1}} = w_{k-1},$$
$$\frac{z}{v_1 v_2 v_3 \ldots v_k} = w_k,\ \ldots\ \frac{z}{v_1 v_2 v_3 \ldots v_n} = \frac{z}{u} = w_n$$

setzt, alle die Quotienten w *ganze* Zahlen.

C. Die beiden vorletzten Gleichungen in (3.) geben, wenn man sie, die erste mit $v_1 v_2 v_3 \ldots v_{k-1}$, die zweite mit $v_1 v_2 v_3 \ldots v_k$ multiplicirt, zufolge (§. 13. *I.*)

$$4.\quad z = v_1 v_2 v_3 \ldots v_{k-1} w_{k-1} \text{ und}$$
$$5.\quad z = v_1 v_2 v_3 \ldots v_{k-1} v_k w_k,$$

also, (4.) durch (5.) dividirt,

$$6.\quad \frac{z}{z} = 1 = \frac{v_1 v_2 v_3 \ldots v_{k-1} w_{k-1}}{v_1 v_2 v_3 \ldots v_{k-1} v_k w_k} = \frac{w_{k-1}}{v_k w_k} \text{ (§. 13. } I.\text{)},$$

und dieses mit w_k multiplicirt, wiederum nach (§. 13. *I.*),

$$7.\quad \frac{w_{k-1}}{v_k} = w_k.$$

D. Da nun k jede der Zahlen 1, 2, 3, ... n sein kann, so giebt (7.)

$$8.\quad \frac{w_1}{v_2} = w_2,\quad \frac{w_2}{v_3} = w_3,\quad \frac{w_3}{v_4} = w_4,\ \ldots\ \frac{w_{n-1}}{v_n} = w_n.$$

Hieraus folgt

Erstlich, dafs jeder der Quotienten w der Division von z durch die Factoren v von u (3.) durch einen derjenigen Factoren v von u *theilbar* ist, die bis dahin noch nicht zur Division gekommen sind; denn die sämmtlichen Quotienten in (8.) sind ganze Zahlen (***B.***). So behauptet es der Lehrsatz.

Zweitens, dafs, wenn man zuerst z durch v_1 dividirt, welches den Quotienten w_1 giebt (3.), darauf diesen Quotienten w_1 durch v_2, den daraus nach (8.) hervorgehenden Quotienten w_2 durch v_3 u. s. w. bis *alle* Factoren v von u zur Division gelangt sind: dafs dann der *letzte* Quotient w_n der *nemliche* ist, welcher sich zufolge (3.) ergiebt, wenn man z *auf einmal* durch $v_1 v_2 v_3 \ldots v_n = u$ dividirt; dem Lehrsatze gemäfs.

E. Übrigens ist es gleichgültig, in welcher ***Ordnung*** die Factoren v von u bei dem zweiten Divisionsverfahren zur Division gelangen, da die Factoren v_1, v_2, v_3, ... v_n von u zufolge (§. 6.) nach Belieben *verwechselt* werden dürfen. Auch ändert sich an dem Beweise nichts, die Fac-

toren v von u mögen, einige oder alle, unter einander gleich oder ungleich sein; was die übrigen Behauptungen des Lehrsatzes sind.

Anm. Der Beweis ergiebt sich insbesondere aus der *Vergleichung* in (*C.*) zweier Quotienten w von z, dividirt durch Factoren von u, in welchen der Divisor des einen *einen* Factor von u mehr enthält, als der andere.

§. 17.

Lehrsatz.

Der Lehrsatz (§. 16.) von der Gleichheit der Endresultate, es mag eine ganze Zahl z *durch eine andere ganze Zahl* u *auf einmal, oder erst durch irgend einen Factor von* u, *der Quotient davon durch einen zweiten Factor von* u, *der Quotient davon durch einen dritten Factor von* u *dividirt werden u. s. w. bis alle Factoren von* u *erschöpft sind, gilt nicht blofs für den Fall, wenn* u *in* z *aufgeht, sondern auch dann, wenn* u *in* z *nicht aufgeht; jedoch dann nur auf folgende Weise:*

I. *Dividirt man nämlich in diesem Fall* z *zuerst durch irgend einen Factor* v_1 *von* u, *und zwar so, dafs das was bleibt entweder der echte positive oder der echte negative Rest* (§. 8. IV. *a.*) *ist; hierauf den so gefundenen unternächsten oder übernächsten Quotienten* (§. 8. IV. *b.*) *durch irgend einen zweiten Factor* v_2 *von* u, *unter der gleichen Beobachtung; den hieraus hervorgehenden Quotienten durch einen dritten Factor* v_3 *von* u, *wiederum unter derselben Beobachtung, und so weiter bis alle Factoren von* u *erschöpft sind, so kommt man, und zwar immer unter der Bedingung, dafs bei den stufenweisen Divisionen stets entweder der positive oder der negative echte Rest genommen wird (nicht willkürlich bald der eine, bald der andere), zuletzt auf denselben Quotienten, der sich findet, wenn man* z *durch* u *auf einmal dividirt und auch hierbei, eben wie bei den stufenweisen Divisionen, gleichfalls den positiven oder den negativen echten Rest nimmt, je nachdem der eine oder der andere bei den stufenweisen Divisionen genommen wurde.*

Bezeichnet man, indem

$$1.\quad u = v_1 v_2 v_3 \ldots v_n$$

gesetzt wird, die bei den verschiedenen theilweisen Divisionen bleibenden Reste, je nachdem sie die positiven oder die negativen echten Reste sind, durch $r_1, r_2, r_3, \ldots r_n$, *und durch* $\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \ldots \mathfrak{r}_n$, *die zugehöri-*

gen unternächsten und übernächsten Quotienten durch $q_1, q_2, q_3, \ldots q_n$ *und durch* $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \ldots \mathfrak{q}_n$; *ferner den positiven echten Rest der Division von* z *mit* u *durch* R, *den negativen echten Rest dieser Division durch* $\mathfrak{R}$, *die zugehörigen unternächsten und übernächsten Quotienten durch* Q *und* $\mathfrak{Q}$, *so dafs die Gleichungen*

$$2. \begin{cases} z = q_1 v_1 + r_1, \\ q_1 = q_2 v_2 + r_2, \\ q_2 = q_3 v_3 + r_3, \\ q_3 = q_4 v_4 + r_4, \\ \ldots \ldots \\ q_{n-1} = q_n v_n + r_n, \end{cases} \qquad 3. \begin{cases} z = \mathfrak{q}_1 v_1 - \mathfrak{r}_1, \\ \mathfrak{q}_1 = \mathfrak{q}_2 v_2 - \mathfrak{r}_2, \\ \mathfrak{q}_2 = \mathfrak{q}_3 v_3 - \mathfrak{r}_3, \\ \mathfrak{q}_3 = \mathfrak{q}_4 v_4 - \mathfrak{r}_4, \\ \ldots \ldots \\ \mathfrak{q}_{n-1} = \mathfrak{q}_n v_n - \mathfrak{r}_n, \end{cases}$$

und

$$4. \quad z = Qu + R \text{ und}$$

$$5. \quad z = \mathfrak{Q}u - \mathfrak{R}$$

die verschiedenen oben beschriebenen Divisionen vorstellen und die Quotienten q, Q *und* $\mathfrak{q}$, $\mathfrak{Q}$, *durch die Bezeichnungen* (§. 8. IV. *b.*) *ausgedrückt, nichts anderes sind als*

$$6. \begin{cases} q_1 = (z + : v_1), \\ q_2 = ((z + : v_1) + : v_2), \\ q_3 = (((z + : v_1) + : v_2) + : v_3), \\ \ldots \ldots \\ q_n = ((((z + : v_1) + : v_2) + : v_3) \ldots + : v_n), \end{cases}$$

$$7. \quad Q = (z + : u),$$

und

$$8. \begin{cases} \mathfrak{q}_1 = (z - : v_1), \\ \mathfrak{q}_2 = ((z - : v_1) - : v_2), \\ \mathfrak{q}_3 = (((z - : v_1) - : v_2) - : v_3), \\ \ldots \ldots \\ \mathfrak{q}_n = ((((z - : v_1) - : v_2) - : v_3) \ldots - : v), \end{cases}$$

$$9. \quad \mathfrak{Q}_n = (z - : u),$$

so läfst sich das, was bisher von dem Lehrsatze ausgesprochen ist, in Zeichen durch die beiden Gleichungen

$$10. \quad Q = q_n \text{ und}$$

$$11. \quad \mathfrak{Q} = \mathfrak{q}_n,$$

oder auch durch die beiden Gleichungen

12. $(z \dotplus : u) = ((((z \dotplus : v_1) \dotplus : v_2) \dotplus : v_3) \dots\dots \dotplus : v_n)$ *und*

13. $(z \dot{-} : u) = ((((z \dot{-} : v_1) \dot{-} : v_2) \dotplus : v_3) \dots\dots \dot{-} : v_n)$

ausdrücken.

II. ***Wenn*** u ***in*** z ***aufgeht, wie in*** (§. 16.), ***so sind alle Reste*** r, $\mathfrak{r}$, R und $\mathfrak{R}$, ***Null. Hier, wo*** u ***in*** z ***nicht aufgehen soll, sind die Reste nicht Null, sondern*** R ***und*** $\mathfrak{R}$ ***werden wie folgt durch*** r ***und*** $\mathfrak{r}$ ***und durch die Factoren*** v ***von*** u ***ausgedrückt:***

14. $$R = r_n v_1 v_2 v_3 \dots\dots v_{n-1} + r_{n-1} v_1 v_2 v_3 \dots\dots v_{n-2} + r_{n-2} v_1 v_2 v_3 \dots\dots v_{n-3} \dots \dots + r_3 v_1 v_2 + r_2 v_1 + r_1$$ ***und***

15. $$\mathfrak{R} = \mathfrak{r}_n v_1 v_2 v_3 \dots\dots v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \dots\dots v_{n-2} + \mathfrak{r}_{n-2} v_1 v_2 v_3 \dots\dots v_{n-3} \dots \dots + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1,$$

oder auch, wenn man

16. $$v_1 = V_1, \quad v_1 v_2 = V_2, \quad v_1 v_2 v_3 = V_3 \dots\dots v_1 v_2 v_3 \dots\dots v_{n-1} = V_{n-1}$$

setzt, durch

17. $$R = r_n V_{n-1} + r_{n-1} V_{n-2} + r_{n-2} V_{n-3} \dots\dots + r_3 V_2 + r_2 V_1 + r_1$$ ***und***

18. $$\mathfrak{R} = \mathfrak{r}_n V_{n-1} + \mathfrak{r}_{n-1} V_{n-2} + \mathfrak{r}_{n-2} V_{n-3} \dots\dots + \mathfrak{r}_3 V_2 + \mathfrak{r}_2 V_1 + \mathfrak{r}_1.$$

III. a. ***Der letzte Quotient*** $\mathfrak{q}_n$ ***in*** (3.) ***ist gleich dem letzten Quotienten*** q_n ***in*** (2.) ***wenn*** u ***in*** z ***aufgeht. Geht*** u ***in*** z ***nicht auf, so ist***

19. $$\mathfrak{q}_n = q_n + 1.$$

b. ***Läfst man in*** (3.) ***die Factoren*** v ***und*** u ***in derselben Ordnung auf einander folgen, wie in*** (2.), ***so kann keiner der Quotienten*** q ***gröfser sein, als der ihm correspondirende Quotient*** $\mathfrak{q}$, ***sondern nur entweder ihm gleich, oder um*** 1 ***kleiner.***

c. ***Geht der erste Factor*** v_1 ***von*** u ***in*** z ***nicht auf, so sind alle Quotienten*** $\mathfrak{q}$ ***jeder um*** 1 ***gröfser, als die correspondirenden Quotienten*** $\mathfrak{q}$.

d. ***Geht der erste Factor*** v_1 ***von*** u ***in*** z ***auf, desgleichen der zweite Factor*** v_2 ***in den ersten Quotienten*** q_1, ***der dritte Factor*** v_3 ***in den zweiten Quotienten*** q_2 ***u. s. w. bis zum mten Factor*** v_m ***von*** u, ***so sind die Quotienten*** $q_1, q_2, q_3, \dots\dots q_m$ ***alle den Quotienten*** $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \dots\dots \mathfrak{q}_m$ ***gleich; alle folgenden Quotienten*** $\mathfrak{q}$ ***dagegen sind sämmtlich jeder um*** 1 ***gröfser als die correspondirenden Quotienten*** q.

Beispiel. Es sei

20. $z = 17017$ und $u = 360 = 2.2.2.3.3.5.$

a. Man nehme zuerst zu Factoren *v* von *u* folgende:

21. $v_1 = 2, \quad v_2 = 2, \quad v_3 = 2, \quad v_4 = 3, \quad v_5 = 3, \quad v_6 = v_n = 5,$

so geben die Gleichungen (2. u. 3.)

$$22.\quad \begin{cases} 17017 = 8508.2+1, \\ 8508 = 4254.2+0, \\ 4254 = 2127.2+0, \\ 2127 = 709.3+0, \\ 709 = 236.3+1, \\ 236 = 47.5+1, \end{cases} \qquad 23.\quad \begin{cases} 17017 = 8509.2-1, \\ 8509 = 4255.2-1, \\ 4255 = 2128.2-1, \\ 2128 = 710.3-2, \\ 710 = 237.3-1, \\ 237 = 48.5-3. \end{cases}$$

Es ist also

$$24.\ \begin{cases} q_1 = 8508, \quad q_2 = 4254, \quad q_3 = 2127, \quad q_4 = 709, \quad q_5 = 236, \quad q_6 = q_n = 47, \\ r_1 = 1, \quad r_2 = 0, \quad r_3 = 0, \quad r_4 = 0, \quad r_5 = 1, \quad r_6 = r_n = 1. \end{cases}$$

$$25.\ \begin{cases} \mathfrak{q}_1 = 8509, \quad \mathfrak{q}_2 = 4255, \quad \mathfrak{q}_3 = 2128, \quad \mathfrak{q}_4 = 710, \quad \mathfrak{q}_5 = 237, \quad \mathfrak{q}_6 = \mathfrak{q}_n = 48, \\ \mathfrak{r}_1 = 1, \quad \mathfrak{r}_2 = 1, \quad \mathfrak{r}_3 = 1, \quad \mathfrak{r}_4 = 2, \quad \mathfrak{r}_5 = 1, \quad \mathfrak{r}_6 = \mathfrak{r}_n = 3; \end{cases}$$

desgleichen giebt hier (4. u. 5.)

$$26.\quad 17017 = 47.360+97 \text{ und}$$

$$27.\quad 17017 = 48.360-263,$$

also ist

$$28.\quad Q = 47, \quad R = 97,$$

$$29.\quad \mathfrak{Q} = 48, \quad \mathfrak{R} = 263.$$

Aus (24. und 28.) und aus (25. und 29.) zeigt sich, dafs, wie es nach (10. und 11.) sein soll, $Q = q_n$ (= 47) und $\mathfrak{Q} = \mathfrak{q}_n$ (= 48) ist.

Ferner ist nach (16. und 21.)

$$30.\quad V_1 = v_1 = 2, \quad V_2 = v_1 v_2 = 4, \quad V_3 = v_1 v_2 v_3 = 8, \quad V_4 = v_1 v_2 v_3 v_4 = 24,$$
$$V_5 = v_1 v_2 .. v_5 = 72, \quad V_6 = v_1 v_2 \ldots v_6 = 360,$$

also geben hier (17. und 18.), gemäfs (30. 24. und 25.),

$$31.\quad R = 1.72+1.24+0.8+0.4+0.2+1 = 72+24+1 = 97 \text{ (wie 28.) und}$$

$$32.\quad \mathfrak{R} = 3.72+1.24+2.8+1.4+1.2+1$$
$$= 216+24+16+4+2+1 = 263 \text{ (wie 29.)}.$$

Desgleichen sieht man aus (24. und 25.), dafs es sich mit den q und $\mathfrak{q}$ so verhält wie es der Lehrsatz in (III. *a. b. c.*) behauptet.

b. Nimmt man zu den Factoren v von u folgende:

$$33.\quad v_1 = 12, \quad v_2 = 5, \quad v_3 = v_n = 6,$$

so geben die Gleichungen (2. und 3.)

$$34.\ \begin{cases} 17017 = 1418.12+1, \\ 1418 = 283.\ 5+3, \\ 283 = 47.\ 6+1; \end{cases} \text{ und } 35.\ \begin{cases} 17017 = 1419.12-11, \\ 1419 = 284.\ 5-1, \\ 284 = 48.\ 6-4; \end{cases}$$

und es ist hier

36. $\begin{cases} q_1 = 1418, & q_2 = 283, & q_3 = q_n = 47, \\ r_1 = 1, & r_2 = 3, & r_3 = r_n = 1; \end{cases}$

37. $\begin{cases} \mathfrak{q}_1 = 1419, & \mathfrak{q}_2 = 284, & \mathfrak{q}_3 = \mathfrak{q}_n = 48, \\ \mathfrak{r}_1 = 11, & \mathfrak{r}_2 = 1, & \mathfrak{r}_3 = \mathfrak{r}_n = 4. \end{cases}$

Also ist zunächst wieder aus (36. und 28., 37. und 29.) $q_n = Q_n$ ($=47$) und $\mathfrak{q}_n = \mathfrak{Q}_n$ ($=48$).

Sodann ist hier

38. $V_1 = v_1 = 12$, $V_2 = v_1 v_2 = 60$ und $V_3 = u = 360$,

und (17. und 18.) geben nach (38. 37. und 36.)

39. $R = 1.60 + 3.12 + 1 = 60 + 36 + 1 = 97$ (wie 28.) und

40. $\mathfrak{R} = 4.60 + 1.12 + 11 = 240 + 12 + 11 = 263$ (wie 29.).

Alle $\mathfrak{q}$ (37.) sind wieder, gemäfs (III.), um 1 gröfser, als die correspondirenden q.

Beweis *A.* Man substituire die *zweiten* der Gleichungen (2. und 3.) in die *ersten*, so erhält man

41. $z = q_2 v_1 v_2 + r_2 v_1 + r_1$ und

42. $z = \mathfrak{q}_2 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1$.

Hierin setze man die Werthe von q_2 und $\mathfrak{q}_2$ aus den *dritten* der Gleichungen (2. und 3.), so ergiebt sich

43. $Z = q_3 v_1 v_2 v_3 + r_3 v_1 v_2 + r_2 v_1 + r_1$ und

44. $Z = \mathfrak{q}_3 v_1 v_2 v_3 - \mathfrak{r}_3 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1$.

Setzt man hierin weiter die Werthe von q_3 und $\mathfrak{q}_3$ aus den *vierten* der Gleichungen (2. und 3.), in das was sich ergiebt die Werthe von q_4 und $\mathfrak{q}_4$ aus den *fünften* der Gleichungen, und so weiter, bis zu q_n und $\mathfrak{q}_n$ aus den *letzten* der Gleichungen (2. und 3.), so erhält man

45. $Z = q_n v_1 v_2 v_3 \dots v_n + r_n v_1 v_2 v_3 \dots v_{n-1} + r_{n-1} v_1 v_2 v_3 \dots v_{n-2} \dots$
$\dots + r_3 v_1 v_2 + r_2 v_1 + r_1$ und

46. $Z = \mathfrak{q}_n v_1 v_2 v_3 \dots v_n - \mathfrak{r}_n v_1 v_2 v_3 \dots v_{n-1} - \mathfrak{r}_{n-1} v_1 v_2 v_3 \dots v_{n-2} \dots$
$\dots - \mathfrak{r}_3 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1$, oder auch

47. $Z = q_n u + [r_n v_1 v_2 v_3 \dots v_{n-1} + r_{n-1} v_1 v_2 v_3 \dots v_{n-2} \dots$
$\dots + r_3 v_1 v_2 + r_2 v_1 + r_1]$ und

48. $Z = \mathfrak{q}_n u - [\mathfrak{r}_n v_1 v_2 v_3 \dots v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \dots v_{n-2} \dots$
$\dots + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1]$.

B. Nun sind, wenn in (2. und 3) z. B. v_1 in z *aufgeht,* die echten Reste r_1 und $\mathfrak{r}_1$ gleich *Null* und die Quotienten q_1 und $\mathfrak{q}_1$ sind einander *gleich.* Geht auch v_2 in q_1 *auf,* so sind die Reste r_2 und $\mathfrak{r}_2$ *Null,* und auch die Quotienten q_n und $\mathfrak{q}_n$ sind einander gleich. Und so weiter.

Geht dagegen v_1 in z *nicht auf*, so sind die Reste r_1 und $\mathfrak{r}_1$ *nicht Null;* aber sie können auch *nicht gröſser* sein als v_1-1 (§. 9. II.), und der Quotient $\mathfrak{q}_1$ ist um 1 gröſser als der Quotient q_1 (§. 9. VII.). Geht v_2 in q_1 *nicht auf*, so sind die Reste r_2 und $\mathfrak{r}_2$ nicht Null und können *nicht gröſser* sein als v_2-1, und $\mathfrak{q}_2$ ist um 1 gröſser als q_2. Und so weiter.

In *keinem* Fall also ist $r_1 > v_1-1$, $r_2 > v_2-1$, $r_3 > v_3-1$, ... $r_n > v_n-1$ und $\mathfrak{r}_1 > v_1-1$, $\mathfrak{r}_2 = v_2-1$, $\mathfrak{r}_3 = v_3-1$, ... $\mathfrak{r}_n = v_n-1$. Die r und $\mathfrak{r}$ können zum Theil oder alle *Null* sein, aber die *gröſsten* Werthe, welche sie haben können, sind v_1-1, v_2-1, v_3-1, ... v_n-1.

C. Die *kleinsten* Werthe also Dessen, was in (47.) mit $q_n u$ durch das Pluszeichen und in (48.) mit $\mathfrak{q}_n u$ durch das Minuszeichen verbunden ist, sind *Null*, die *gröſsten* Werthe dagegen sind in (47. und 48.) *gleichmäſsig*

49. $(v_n-1)v_1v_2v_3\ldots v_{n-1}+(v_{n-1}-1)v_1v_2v_3\ldots v_{n-2}+(v_{n-3}-1)v_1v_2v_3\ldots v_{n-3}\ldots$
$\ldots+(v_3-1)v_1v_2+(v_2-1)v_1+v_1-1,$

und Dieses thut, wenn man die angezeigten Multiplicationen ausführt,

$$\begin{aligned}&v_1v_2v_3\ldots v_n+v_1v_2v_3\ldots v_{n-1}+v_1v_2v_3\ldots v_{n-2}\ldots+v_1v_2v_3+v_1v_2+v_1\\&-v_1v_2v_3\ldots v_{n-1}-v_1v_2v_3\ldots v_{n-2}\ldots-v_1v_2v_3-v_1v_2-v_1-1\\&=v_1v_2v_3\ldots v_n-1\end{aligned}$$

50. $=u-1$.

Jedenfalls also sind die Summen der Glieder, die in (47. und 48.) mit $q_n u$ durch das Pluszeichen und mit $\mathfrak{q}_n u$ durch das Minuszeichen verbunden sind, *nicht kleiner als Null* und *nicht gröſser als* $u-1$.

Bezeichnet man demnach diese Summen durch s und σ, so daſs in (47. und 48.)

51. $z=q_n u+s$ und

52. $z=\mathfrak{q}_n u-\sigma$

ist, so ist s ein *echter positiver* Rest und σ ein *echter negativer* Rest der Division von z durch u; denn diese Reste haben jene Eigenschaft (§. 9. II.). q_n und $\mathfrak{q}_n$ sind die *Quotienten* der Division.

D. Dividirt man dagegen z durch u *auf einmal* und nimmt die *echten positiven und negativen* Reste, so erhält man nach (4. und 5.)

53. $z=Qu+R$ und

54. $z=\mathfrak{Q}u-\mathfrak{R}$.

Es giebt aber bei jeder Division *nur einen* echten positiven und *nur einen* echten negativen Rest: also muſs nothwendig

55. $R=s$ und $\mathfrak{R}=\sigma$

und mithin zufolge (51. und 53.) und (52. und 54.)

56. $q_n u + R = Qu + R$ und $\mathfrak{q}_n u - \mathfrak{R} = \mathfrak{Q}_n u - \mathfrak{R}$

sein; und daraus folgt $q_n u = Qu$ und $\mathfrak{q}_n u = \mathfrak{Q}_n u$, also

57. $q_n = Q$ und

58. $\mathfrak{q}_n = \mathfrak{Q}$;

wie es der Lehrsatz in (10. u. 11.) behauptet.

E. Aus den Werthen von s und σ in (47. u. 48.), die zufolge (55.) $= R$ und $\mathfrak{R}$ sind, folgt

59. $R = r_n v_1 v_2 v_3 \ldots v_{n-1} + r_{n-1} v_1 v_2 v_3 \ldots v_{n-2} + \ldots + r_3 v_1 v_2 + r_2 v_1 + r_1$

und

60. $\mathfrak{R} = \mathfrak{r}_n v_1 v_2 v_3 \ldots v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \ldots v_{n-2} + \ldots + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1$;

welches die Ausdrücke (14. u. 15.) des Lehrsatzes sind.

F. Da in *allen* Fällen $q_n = Q$ und $\mathfrak{q}_n = \mathfrak{Q}$ und, wenn u in z aufgeht, also R und $\mathfrak{R}$ Null sind, zufolge (4. u. 5) $Q = \mathfrak{Q}$, hingegen wenn u in z nicht aufgeht, $\mathfrak{Q} = Q + 1$ ist (§. 9. VII.), so ist auch, wenn u in z aufgeht, $q_n = \mathfrak{q}_n$, und wenn u nicht in z aufgeht, $\mathfrak{q}_n = q_n + 1$; gemäfs (19.).

G. Was für u oder V_n (16.) gilt, gilt nothwendig auch für ein Product V_m *nicht aller* v, sondern nur einer beliebigen Anzahl m der Factoren v von u. Also auch, wenn man einerseits der Reihe nach mit den in V_m enthaltenen m Factoren dividirt, was auf die Quotienten q_m und $\mathfrak{q}_m$ führt, anderseits z auf einmal durch V_m, was die Quotienten Q_m und $\mathfrak{Q}_m$ giebt, kann nur, wie in (10. u. 11.),

61. $Q_m = q_m$ und $\mathfrak{Q}_m = \mathfrak{q}_m$,

oder, wie in (III. *a.*),

62. $\mathfrak{q}_m = q_m$ oder $\mathfrak{q}_m = q_m + 1$

sein. Da nun m jede der Zahlen 1, 2, 3, ... n sein kann, und folglich q_m und $\mathfrak{q}_m$ alle die Quotienten q und $\mathfrak{q}$ in (2. und 3.) ausdrücken, so folgt, dafs kein q gröfser sein kann als das ihm correspondirende $\mathfrak{q}$, sondern nur ihm gleich, oder um 1 kleiner; wie es (III. *b.*) behauptet.

H. Geht der *erste* Factor v_1 von u, mit welchem man z dividirt, in z *nicht auf*, so ist $\mathfrak{q}_1 = q_1 + 1$ (§. 9. VII.). Aber, wenn v_1 in z nicht aufgeht, geht auch $V_m = v_1 v_2 v_3 \ldots v_m$, für eine beliebige Zahl m von Factoren v, in z nicht auf (§. 15. I.). Also ist für die Quotienten $\mathfrak{Q}_m$ und Q_m der Division von z durch V_m, $\mathfrak{Q}_m = Q_m + 1$ (§. 9. VII.). Es ist aber *immer* $\mathfrak{q}_m = \mathfrak{Q}_m$ und $q_m = Q_m$ (61.), also ist auch nothwendig

63. $\mathfrak{q}_m = q_m + 1$.

Hieraus folgt, da m jede der Zahlen 1, 2, 3, ... n sein kann, dafs, wenn der *erste* Factor v_1 von u in z nicht aufgeht, *alle* Quotienten $\mathfrak{q}$ jeder um 1 gröfser sind als die correspondirenden Quotienten q. Dies behauptet (III. *c.*).

I. Geht $V_m = v_1 v_2 v_3 \ldots . v_m$ in z auf, so gehen, nach (§. 15. II.), auch alle die Factoren $V_{m-1} = v_1 v_2 v_3 \ldots . v_{m-1}$, $V_{m-2} = v_1 v_2 v_3 \ldots . v_{m-2}$, ... $V_2 = v_1 v_2$ und $V_1 = v_1$ von V_m in z auf. Also sind alle die Quotienten Q_m, Q_{m-1}, Q_{m-2}, ... Q_1 den Quotienten $\mathfrak{Q}_m$, $\mathfrak{Q}_{m-1}$, $\mathfrak{Q}_{m-2}$, ... $\mathfrak{Q}_1$ der Reihe nach gleich; und da Q *immer* gleich q und $\mathfrak{Q}$ *immer* gleich $\mathfrak{q}$ ist, so sind auch die Quotienten q_m, q_{m-1}, ... q_1 der Reihe nach den Quotienten $\mathfrak{q}_m$, $\mathfrak{q}_{m-1}$, ... $\mathfrak{q}_1$ gleich.

Der hier vorausgesetzte Fall, dafs $V_m = v_1 v_2 v_3 \ldots . v_m$ in z *aufgeht*, ist aber *der*, wenn zuerst v_1 in z aufgeht, darauf v_2 in den Quotienten $q_1 = \frac{z}{v_1}$, v_3 in den Quotienten $q_2 = \frac{q_1}{v_2}$ u. s. w.: denn z enthält alsdann nothwendig alle die Factoren v_1, v_2, v_3, ... v_m, also $\frac{z}{v_1} = q_1$ noch die Factoren v_2, v_3, ... v_m, $\frac{q_1}{v_2} = q_2$ noch die Factoren v_3, v_4, ... v_m u. s. w. Also, wenn v_1 in z aufgeht, v_2 in $q_1 = \frac{z}{v_1}$, v_3 in $q_2 = \frac{q_1}{v_2}$, und so weiter bis zu q_m, so sind alle die Quotienten q_1, q_2, q_3, ... q_m der Reihe nach den Quotienten $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\mathfrak{q}_3$, ... $\mathfrak{q}_m$ *gleich.*

Geht $V_{m+1} = v_1 v_2 v_3 \ldots . v_m v_{m+1}$ nicht mehr in z auf, so gehen, gemäfs (§. 15. I.), auch V_{m+2}, V_{m+3}, ... V_n nicht in z auf, und dann gilt für die mit V_{m+1}, V_{m+2}, ... V_n correspondirenden Quotienten q_{m+1}, q_{m+2}, ... q_n und $\mathfrak{q}_{m+1}$, $\mathfrak{q}_{m+2}$, ... $\mathfrak{q}_n$ wieder das, was sich in (*H.*) fand, nemlich, dafs alle $\mathfrak{q}$ um 1 gröfser sind, als die correspondirenden q.

Dieses zusammengenommen ist, was (III. *d.*) behauptet.

Anm. Der Beweis von (I. u. II.) des Lehrsatzes, von (*A.* bis *F.*), beruht insbesondere auf dem Umstande, dafs, wie es die Rechnung mit Hülfe von (§. 9.) ergiebt, die Summen der in (47. u. 48.) mit $q_n u$ und $\mathfrak{q}_n u$ durch + und — verbundenen Glieder nicht kleiner als Null und nicht gröfser als $u-1$ sein können. Der Beweis von (III.) des Lehrsatzes, von (*G.* bis *I.*), nimmt (§. 9. u. 15.) zu Hülfe und beruht nächstdem darauf, dafs das, was für $u = V_n$ gilt, auch für V_m gelten mufs; wo m jede Zahl von 1 bis n sein kann.

§. 18.

Lehrsatz.

Wenn $z_1, z_2, z_3, \ldots z_n$ *beliebige positive oder negative ganze Zahlen sind, und es ist*

$$1. \quad z_1 + z_2 + z_3 \ldots + z_{n-1} = z_n,$$

oder auch, da die z *sowohl positiv als negativ sollen sein können,*

$$2. \quad z_1 + z_2 + z_3 \ldots z_{n-1} + z_n = 0,$$

so geht jede ganze Zahl, welche Gemeintheiler aller z *bis auf eines ist, auch noch in dieses eine auf und ist folglich ein Gemeintheiler aller.*

Beweis. Einer der Gemeintheiler z. B. von $z_1, z_2, z_3, \ldots z_{n-1}$ sei die ganze Zahl u und es sei

$$3. \quad \frac{z_1}{u} = w_1, \quad \frac{z_2}{u} = w_2, \quad \frac{z_3}{u} = w_3, \quad \ldots \quad \frac{z_{n-1}}{u} = w_{n-1}, \quad \frac{z_n}{u} = w_n,$$

so sind *nach der Voraussetzung* $w_1, w_2, w_3, \ldots w_{n-1}$ sämmtlich *ganze* Zahlen.

Dividirt man nun die Gleichung (1.) mit u, so ergiebt sich

$$4. \quad \frac{z_1}{u} + \frac{z_2}{u} + \frac{z_3}{u} \ldots + \frac{z_{n-1}}{u} = \frac{z_n}{u},$$

also, wenn (3.) in (1.) substituirt wird,

$$5. \quad w_1 + w_2 + w_3 \ldots + w_{n-1} = w_n = \frac{z_n}{u}.$$

Aber $w_1, w_2, w_3, \ldots w_{n-1}$ sind sämmtlich *ganze* Zahlen, und die Verbindung ganzer positiver oder negativer Zahlen durch Zusammenzählen ist ebenfalls eine ganze Zahl. Also ist vermöge (5.) nothwendig auch $w_n = \frac{z_n}{u}$ eine *ganze* Zahl, und folglich geht nothwendig der Gemeintheiler u aller z, bis auf das eine z_n, auch in dieses eine auf (§. 14. III.), und ist folglich ein Gemeintheiler *aller z*.

§. 19.

Lehrsatz.

Von zwei beliebigen theilbaren oder untheilbaren, ungleichen ganzen Zahlen sei z_1 *die gröfsere,* z_2 *die kleinere. Man dividire* z_1 *durch* z_2 *und nehme den echten positiven oder negativen Rest* r, *dessen Werth zeichenfrei also* $< z_2$ *ist, oder auch den unbedingt echten oder*

den *kleinsten Rest.* *Hierauf dividire man die kleinere Zahl* z_2 *durch den Rest* r_1 *und nehme wieder beliebig den echten positiven oder negativen oder den kleinsten Rest* r_2, *dessen Werth zeichenfrei also* $< r_1$ *ist. Man dividire* r_1 *durch* r_2 *auf gleiche Weise und nehme den Rest* r_3, *der* $< r_2$ *ist. Man dividire* r_2 *durch* r_3 *auf gleiche Weise und nehme den Rest* r_4, *der* $< r_3$ *ist. Fährt man so immer weiter fort, so ergiebt sich Folgendes.*

I. *Zuletzt kommt man immer nothwendig auf einen Rest* r_n, *welcher Null ist.*

II. *Der vorletzte Rest* r_{n-1} *ist immer der gröfste Gemeintheiler von* z_1 *und* z_2, *so wie von* z_2 *und* r_1, *und von allen auf einander folgenden Paaren von Resten; desgleichen von der Gesammtheit der Zahlen* $z_1, z_2, r_1, r_2, r_3, \ldots r_{n-1}$, *nicht aber nothwendig von zweien oder mehreren unter ihnen, die nicht unmittelbar auf einander folgen. Diese können auch gröfsere Gemeintheiler haben.*

III. *Ist der vorletzte Rest* r_{n-1} *gleich* 1, *so sind die zwei Zahlen* z_1 *und* z_2, *desgleichen* z_2 *und der erste Rest* r_1, *so wie auch alle je zwei auf einander folgenden Reste nothwendig theilerfremd; desgleichen ist dann die Gesammtheit der Zahlen* $z_1, z_2, r_1, r_2, \ldots r_{n-1}$ *gemeintheilerfremd; nicht aber sind nothwendig zwei oder mehrere dieser Zahlen, die nicht unmittelbar auf einander folgen, theilerfremd.*

IV. *Sind umgekehrt die beiden Zahlen* z_1 *und* z_2 *theilerfremd, so ist der vorletzte Rest* r_{n-1} *nothwendig gleich* 1; *und auch* z_2 *und der erste Rest* r_1, *sammt allen Paaren auf einander folgender Reste, jedoch nicht nothwendig die nicht unmittelbar auf einander folgenden, sind theilerfremd. Gemeintheilerfremd aber ist die Gesammtheit der Zahlen* $z_1, z_2, r_1, r_2, \ldots r_{n-1}$.

V. *Sind die beiden Zahlen* z_1 *und* z_2 *theilerverwandt, und man dividirt sie, so wie alle Reste* r, *mit ihrem gröfsten Gemeintheiler, der nach* (II.) *der vorletzte Rest* r_{n-1} *ist, welcher in sie allein aufgeht, so gilt von den Quotienten derselben, was in dem Falle* (IV.) *von den Zahlen* $z_1, z_2, r_1, r_2, \ldots r_{n-1}$ *selbst gilt.*

Beweis I. *A*. Die verschiedenen in dem Satz beschriebenen Divisionen werden durch

$$1.\quad \begin{cases} z_1 = \mathfrak{S} z_2 \pm r_1, \\ z_2 = \mathfrak{S} r_1 \pm r_2, \\ r_1 = \mathfrak{S} r_2 \pm r_3, \\ r_2 = \mathfrak{S} r_3 \pm r_4, \\ \dots\dots\dots\dots \\ r_{n-4} = \mathfrak{S} r_{n-3} \pm r_{n-2}, \\ r_{n-3} = \mathfrak{S} r_{n-2} \pm r_{n-1}, \\ r_{n-2} = \mathfrak{S} r_{n-1} \pm r_n \end{cases}$$

ausgedrückt, wo die r die ***zeichenfreien Zahlenwerthe*** der ***Reste*** bezeichnen, für welche dann nach Belieben die Zeichen $+$ oder $-$ gelten können.

B. Die ***zeichenfreien*** Zahlenwerthe, welche die r ausdrücken, sind, selbst dann, wenn man nicht die ***unbedingt echten*** Reste nimmt, jedenfalls ***kleiner*** als die zugehörigen Divisoren, da die r jedenfalls ***echte*** Reste sein sollen; das heifst: es ist, den ***zeichenfreien*** Zahlenwerthen nach,

$$2.\quad r_1 < z_2,\quad r_2 < r_1,\quad r_3 < r_2,\quad r_4 < r_3,\ \dots$$

C. Die zeichenfreien Zahlenwerthe von r_1, r_2, r_3, ... nehmen daher nothwendig ***immer fort ab;*** keiner kann ***gröfser*** als der vorhergehende, oder auch nur ihm ***gleich*** sein, sondern ***nur kleiner;*** also wenigstens um 1. Daraus folgt, dafs man zuletzt nothwendig auf einen Rest r_n kommen mufs, der ***Null*** ist. Denn wie klein auch schon der zeichenfreie Zahlenwerth eines r sein mag: es kann, wenn dieser Werth noch nicht Null sein sollte, durch fortgesetzte Division ein ***noch kleineres r*** hervorgebracht werden; so lange, bis die Grenze 0 der Kleinheit erreicht ist. Dieses ist was (I.) behauptet.

Beweis von II. ***D.*** Da zufolge (I.) der letzte Rest r_n ***immer*** nothwendig Null ist, so reducirt sich die ***letzte*** der Gleichungen (I.) ***immer*** auf

$$3.\quad r_{n-2} = \mathfrak{S} r_{n-1},$$

welches ausdrückt, dafs r_{n-2} ein ***Vielfaches*** von r_{n-1}, nemlich das $\mathfrak{S}$***fache*** von r_{n-1} ist und dafs also r_{n-1} in r_{n-2} ***aufgeht.*** Also ist r_{n-1} ein ***Gemeintheiler*** von r_{n-1} und r_{n-2}, und zwar der ***gröfste*** Gemeintheiler, da in r_{n-1} keine ***gröfsere*** Zahl aufgehen kann, als ***sie selbst.***

E. Hieraus folgt, vermöge der ***vorletzten*** Gleichung in (1.) und vermöge (§. 18.), dafs r_{n-1} auch in r_{n-3} aufgehen mufs. Denn da es in den beiden ganzen Zahlen r_{n-1} und r_{n-2} aufgeht, so mufs es vermöge jener vorletzten Gleichung

$$4.\quad r_{n-3} = \mathfrak{S} r_{n-2} + r_{n-1}$$

zufolge (§. 18.) auch in die ganze Zahl r_{n-3} aufgehen. Also ist r_{n-1} auch

ein *Gemeintheiler* von r_{n-2} und r_{n-3}, und zwar der *gröſste;* denn hätten r_{n-3} und r_{n-2} einen gröſsern Gemeintheiler als r_{n-1}, so müſste derselbe, vermöge *derselben* Gleichung (4.) zufolge (§. 18.) auch in r_{n-1} aufgehen; was nicht möglich ist, da keine Zahl in eine *kleinere* aufgeht.

F. Daraus, daſs r_{n-1} der *gröſste Gemeintheiler* von r_{n-3} und r_{n-2} ist, folgt weiter, vermöge der vorvorletzten Gleichung (1.), nemlich aus

$$6. \quad r_{n-4} = \mathfrak{G} r_{n-3} + r_{n-2}$$

und aus (§. 18.), daſs r_{n-1} auch in r_{n-4} aufgehen und also, eben so wie von r_{n-2} und r_{n-3}, auch von r_{n-3} und r_{n-4} ein *Gemeintheiler* sein muſs, und zwar wiederum der *gröſste;* denn hätte r_{n-3} und r_{n-4} einen gröſseren Gemeintheiler als r_{n-1}, so müſste derselbe vermöge der nemlichen Gleichung (6.) und (§. 18.) auch in r_{n-2} aufgehen; also hätten r_{n-3} und r_{n-2} einen gröſsern Gemeintheiler als r_{n-1}; was nach (*E.*) nicht der Fall ist.

G. Auf ganz gleiche Weise folgt aus den weiter vorhergehenden Gleichungen in (1.), daſs r_{n-1} auch der *gröſste Gemeintheiler* von r_{n-4} und r_{n-5}, von r_{n-5} und r_{n-6} u. s. w. und zuletzt von r_1 und r_2 ist. Sodann folgt aus der zweiten der Gleichungen (1.), und immer aus gleichen Gründen, daſs r_{n-1} auch der gröſste Gemeintheiler von z_2 und r_1 ist, und aus der *ersten* der Gleichungen (1.), daſs r_{n-1} nicht minder der *gröſste Gemeintheiler* von z_1 und z_2 ist.

Der *vorletzte Rest* r_{n-1} ist also *immer,* unter allen Umständen, der *gröſste Gemeintheiler* von z_1 und z_2, so wie von z_2 und r_1, von r_1 und r_2 von r_2 und r_3, und überhaupt von jedem Paare *unmittelbar aufeinander folgender* Reste.

H. Daraus folgt ferner, daſs r_{n-1} in *allen* den Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} *zugleich* aufgeht, und daſs es also *ein Gemeintheiler* derselben, und zwar der *gröſste* ist, da in der *letzten* dieser Zahlen r_{n-1} keine gröſsere Zahl aufgehen kann, als sie selbst.

Es kann aber allerdings *gröſsere* Theiler als r_{n-1} geben, die in zwei oder mehrere *nicht* unmittelbar auf einander folgende Reste aufgehen. Denn wenn es auch keinen gröſsern Theiler als r_{n-1} giebt, der z. B. in r_2 und r_3 zugleich aufgeht, so kann es doch einen gröſsern Gemeintheiler von r_2 und $\mathfrak{G}$*mal* r_3 geben, welcher, der Gleichung $r_2 = \mathfrak{G} r_3 + r_4$ gemäſs, zugleich in r_4 aufgeht u. s. w.

Dieses zusammen ist was (II.) behauptet.

Beweis von III. *I.* Da nach (II.) der vorletzte Rest r_{n-1} der *gröfste* Gemeintheiler von z_1 und z_2, von z_2 und r_1, von r_1 und r_2 und weiter von allen Paaren unmittelbar auf einander folgender Reste ist, so folgt, dafs, in dem Fall wenn $r_{n-1} = 1$ ist, alle die genannten Zahlenpaare mit *keiner gröfsern* Zahl als 1 aufgehen und mithin *theilerfremd* sind. Auch hat jetzt die Gesammtheit der Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} keinen gröfsern *Gemeintheiler* als 1, und ist folglich *gemeintheilerfremd*. Nicht aber sind nothwendig nicht unmittelbar auf einander folgende von jenen Zahlen theilerfremd; aus demselben Grunde wie in (*H.*). Dieses ist was (III.) behauptet.

Beweis von IV. *K.* Sind z_1 und z_2 *theilerfremd,* so sind es vermöge der ersten Gleichung in (1.) auch z_2 und r_1; denn hätten z_2 und r_1 einen gröfsern Gemeintheiler als 1, so müfste derselbe zufolge (§. 18.) auch in z_1 *aufgehen,* und folglich hätten dann z_2 und z_1 einen gröfsern Gemeintheiler als 1; der Voraussetzung entgegen.

L. Daraus, dafs hier z_2 und r_1 nothwendig theilerfremd sind, folgt weiter, vermöge der *zweiten* der Gleichungen (2.), ganz auf dieselbe Weise wie in (*K.*), dafs auch nothwendig r_1 und r_2 theilerfremd sind. Hieraus folgt, vermöge der *dritten* Gleichung (1.), wieder auf dieselbe Weise, dafs auch r_2 und r_3 theilerfremd sind; und so weiter fort, bis zu r_{n-2} und r_{n-1}.

M. Es folgt also zunächst, dafs, wenn z_1 und z_2 theilerfremd sind, das Gleiche auch mit allen den Zahlenpaaren z_2 und r_1, r_1 und r_2, r_2 und r_3 bis zu r_{n-2} und r_{n-1} der Fall ist.

N. Nun ist aber, was auch r_{n-1} sein mag, nach (II.) r_{n-1} *immer* der *gröfste* Gemeintheiler von z_1 und z_2: in dem gegenwärtigen Falle, wo z_1 und z_2 *theilerfremd* sein sollen, *haben* sie keinen gröfsern Gemeintheiler als 1: also ist in diesem Fall auch nothwendig $r_{n-1} = 1$.

Dieses behauptet der Lehrsatz in (IV.). Das Übrige von (IV.) folgt ähnlich wie für (III.).

Beweis von V. *O.* Dividirt man z_1 und z_2 mit ihrem *gröfsten* Gemeintheiler r_{n-1}, der zufolge (II.) zugleich der gröfste Gemeintheiler aller der Zahlenpaare z_2 und r_1, r_1 und r_2, r_2 und r_3 bis zu r_{n-2} und r_{n-1} ist und folglich in sie alle aufgeht, so haben alle die Zahlen nun *keinen* Gemeintheiler mehr; folglich sind alle die *Quotienten* paarweise theilerfremd, und mithin in demselben Falle, wie wenn z_1 und z_2 theilerfremd wären. Also gilt von diesen Quotienten Dasselbe, was in dem Falle (IV.) von den Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} selbst gilt. Dieses behauptet (V.).

Anm. 1. Die Beweise der verschiedenen Theile des Lehrsatzes beruhen insbesondere darauf, dafs, wenn *zwei* Zahlen in einer Gleichung mit *drei Gliedern* einen Theiler gemein haben, derselbe nach (§. 18.) auch in die *dritte* Zahl aufgehen mufs.

Anm. 2. Wenn man den *gröfsten Gemeintheiler* r_{n-1} zweier gegebenen Zahlen z_1 und z_2 nach dem Lehrsatze *ausrechnen* will, so wird man wohl thun, nicht sowohl immer die *echten positiven*, oder immer die *echten negativen* Reste zu nehmen, sondern vielmehr *immer* die *unbedingt echten* oder *kleinsten* Reste. Denn da von jenen nach (§. 9. II.) die zeichenfreien Zahlenwerthe nur nothwendig kleiner als der *ganze Divisor*, von den *unbedingt echten* Resten dagegen die zeichenfreien Zahlenwerthe nach (§. 9. IV.) nothwendig kleiner als die *Hälfte des Divisors* sind, so werden die Reste der verschiedenen Divisionen, wenn man die *kleinsten* Reste nimmt, schneller abnehmen und man wird also damit eher zum Ziele gelangen.

Es sei z. B. $z_1 = 9012$ und $z_2 = 6459$, so ist die Rechnung nach den drei verschiedenen Arten folgende:

$$7.\quad \left\{\begin{array}{rcl} 9012 &=& 1.6459+2553 \\ 6459 &=& 2.2553+1353 \\ 2553 &=& 1.1353+1200 \\ 1353 &=& 1.1200+153 \\ 1200 &=& 7.153+129 \\ 153 &=& 1.129+24 \\ 129 &=& 5.24+9 \\ 24 &=& 2.9+6 \\ 9 &=& 1.6+3 \\ 6 &=& 2.3+0 \end{array}\right.
\qquad
8.\quad \left\{\begin{array}{rcl} 9012 &=& 2.6459-3906 \\ 6459 &=& 2.3906-1353 \\ 3906 &=& 3.1353-153 \\ 1353 &=& 9.153-24 \\ 153 &=& 7.24-15 \\ 24 &=& 2.15-6 \\ 15 &=& 3.6-3 \\ 6 &=& 2.3-0 \end{array}\right.$$

$$9.\quad \left\{\begin{array}{rcl} 9012 &=& 1.6459+2553 \\ 6459 &=& 3.2553-1200 \\ 2553 &=& 2.1200+153 \\ 1200 &=& 8.153-24 \\ 153 &=& 6.24+9 \\ 24 &=& 3.9-3 \\ 9 &=& 3.3+0 \end{array}\right.$$

In (7.) sind durchweg die *positiven echten* Reste, in (8.) die *negativen echten* Reste und in (9.) die *unbedingt echten* Reste genommen. Die letzte

Rechnung ist, wie sich zeigt, die kürzeste. Der *gröfste Gemeintheiler* von z_1 und z_2 und von *allen* Resten $r_1, r_2, r_3, \ldots r_{n-1}$, so wie aller ***Paare unmittelbar*** auf einander folgender Reste ist hier $r_{n-1} = 3$. Aber 3 ist nicht der *gröfste* Gemeintheiler ***nicht unmittelbar*** auf einander folgender Reste. Z. B. die beiden Reste 1200 und 24 in (7. und 9.) haben nicht blofs 3 sondern 24 zum *gröfsten* Gemeintheiler.

§. 20.

Lehrsatz.

I. ***Wenn eine ganze Zahl*** u ***zu jeder der beiden beliebigen ganzen Zahlen*** z_1, z_2 ***theilerfremd ist, so ist sie es auch zu ihrem Producte*** $z_1 z_2$; ***gleichviel ob*** z_1 ***und*** z_2 ***ungleich oder einander gleich, theilerverwandt oder theilerfremd sind.***

II. ***Wenn eine untheilbare oder Stammzahl*** p ***in keine der beiden ganzen Zahlen*** z_1 ***und*** z_2 ***aufgeht, so geht sie auch in ihr Product*** $z_1 z_2$ ***nicht auf, gleichviel, wie vorhin, was*** z_1 ***und*** z_2 ***sein mögen.***

Beispiele. ***No. 1.*** Die Zahl $u = 8$ ist zu jeder der Zahlen $z_1 = 15$ und $z_2 = 21$ theilerfremd: zu dem Product $z_1 z_2 = 15.21 = 315$ ist sie es gleichfalls.

No. 2. Die untheilbare Zahl 11 geht in keine der beiden Zahlen $z_1 = 24$ und $z_2 = 81$ auf; und in ihr Product $z_1 z_2 = 24.81 = 1944$ ebenfalls nicht.

Beweis von I. ***A.*** Die Zahl u kann weder *gleich* z_1 noch *gleich* z_2 sein, denn sonst wäre sie zu z_1 oder zu z_2 nicht *theilerfremd.* Sie kann also nur *kleiner* oder *gröfser* sein, als die eine oder die andere der beiden Zahlen z_1 und z_2, z. B. als z_1.

B. Je nachdem ***u kleiner*** oder *gröfser* ist als z_1, setze man:

$$1.\ \left\{\begin{aligned} z_1 &= \mathfrak{G}u \pm r_1, \\ u &= \mathfrak{G}r_1 \pm r_2, \\ r_1 &= \mathfrak{G}r_2 \pm r_3, \\ r_2 &= \mathfrak{G}r_3 \pm r_4, \\ &\ldots\ldots\ldots\ldots \\ r_{n-4} &= \mathfrak{G}r_{n-3} \pm r_{n-2}, \\ r_{n-3} &= \mathfrak{G}r_{n-2} \pm r_{n-1}, \\ r_{n-2} &= \mathfrak{G}r_{n-1} \pm r_n; \end{aligned}\right. \quad \text{oder} \quad 2.\ \left\{\begin{aligned} u &= \mathfrak{G}z_1 \pm \varrho_1, \\ z_1 &= \mathfrak{G}\varrho_1 \pm \varrho_2, \\ \varrho_1 &= \mathfrak{G}\varrho_2 \pm \varrho_3, \\ \varrho_2 &= \mathfrak{G}\varrho_3 \pm \varrho_4, \\ &\ldots\ldots\ldots\ldots \\ \varrho_{n-4} &= \mathfrak{G}\varrho_{n-3} \pm \varrho_{n-2}, \\ \varrho_{n-3} &= \mathfrak{G}\varrho_{n-2} \pm \varrho_{n-1}, \\ \varrho_{n-2} &= \mathfrak{G}\varrho_{n-1} \pm \varrho_n; \end{aligned}\right.$$

wo die r und die ϱ sämmtlich entweder ***positive,*** oder ***negative,*** oder ***unbedingt echte*** Reste bezeichnen, jedenfalls aber ***echte Reste.***

C. Zufolge (§. 19. I. und IV.) ist hier nothwendig, da z_1 und u theilerfremd vorausgesetzt werden, nächst

$$3.\quad r_n = 0 \quad \text{und} \quad \varrho_n = 0, \text{ auch}$$

$$4.\quad r_{n-1} = \pm 1 \quad \text{und} \quad \varrho_{n-1} = \pm 1,$$

so dafs sich die ***beiden letzten*** Gleichungen in (1. u. 2.) auf

$$5.\ \begin{cases} r_{n-3} = \mathfrak{G} r_{n-2} \pm 1, \\ r_{n-2} = \mathfrak{G}.1 \end{cases} \quad \text{und} \quad 6.\ \begin{cases} \varrho_{n-3} = \mathfrak{G} \varrho_{n-2} \pm 1, \\ \varrho_{n-2} = \mathfrak{G}.1 \end{cases}$$

reduciren.

D. Nun multiplicire man die sämmtlichen Gleichungen (1. und 2.), zugleich auf (5. und 6.) Rücksicht nehmend, mit z_2, so erhält man

$$7.\ \begin{cases} z_1 z_2 = \mathfrak{G} u z_2 \pm r_1 z_2, \\ u z_2 = \mathfrak{G} r_1 z_2 \pm r_2 z_2, \\ r_1 z_2 = \mathfrak{G} r_2 z \pm r_3 z_2, \\ r_2 z_2 = \mathfrak{G} r_3 z_2 \pm r_4 z_2, \\ \dots\dots\dots\dots \\ r_{n-4} z_2 = \mathfrak{G} r_{n-3} z_2 \pm r_{n-2} z_2, \\ r_{n-3} z_2 = \mathfrak{G} r_{n-2} z_2 \pm z_2 \\ r_{n-2} z_2 = \mathfrak{G} z_2; \end{cases} \qquad 8.\ \begin{cases} u z_2 = \mathfrak{G} z_1 z_2 \pm \varrho_1 z_2, \\ z_1 z_2 = \mathfrak{G} \varrho_1 z_2 \pm \varrho_2 z_2, \\ \varrho_1 z_2 = \mathfrak{G} \varrho_2 z_2 \pm \varrho_3 z_2, \\ \varrho_2 z_2 = \mathfrak{G} \varrho_3 z_2 \pm \varrho_4 z_2, \\ \dots\dots\dots\dots \\ \varrho_{n-4} z_2 = \mathfrak{G} \varrho_{n-3} z_2 \pm \varrho_{n-2} z_2, \\ \varrho_{n-3} z_2 = \mathfrak{G} \varrho_{n-2} z_2 \pm z_2, \\ \varrho_{n-2} z_2 = \mathfrak{G} z_2. \end{cases}$$

E. Hätten nun in dem Falle $z_1 > u$, auf welchen sich die Gleichungen (7.) beziehen, u und das ***Product*** $z_1 z_2$ einen ***Gemeintheiler*** $\lambda > 1$, so müfste derselbe vermöge der ***ersten*** der Gleichungen (7.), nach (§. 18.), auch in $r_1 z_2$ ***aufgehen,*** also in $u z_2$ und $r_1 z_2$ ***zugleich,*** mithin vermöge der ***zweiten*** Gleichung (7.), nach (§. 18.), auch in $r_2 z_2$, folglich in $r_1 z_2$ und $r_2 z_2$ ***zugleich,*** folglich auch vermöge der ***dritten*** Gleichung (7.), nach (§. 18.), auch in $r_3 z_2$, und so weiter; folglich zuletzt vermöge der ***vorletzten*** der Gleichungen (7.) auch in z_2, mithin in u und z_2 ***zugleich,*** was der Voraussetzung entgegen ist, also kann ein Gemeintheiler von u und $z_1 z_2$, z. B. λ, ***nicht*** gröfser sein als 1.

F. Hätten in dem Falle $z_1 < u$, auf welchen sich die Gleichungen (8.) beziehen, u und das ***Product*** $z_1 z_2$ einen ***Gemeintheiler*** $z > 1$, so müfste derselbe vermöge der ***ersten*** der Gleichungen (8.), nach (§. 18.), auch in $\varrho_1 z_2$ ***aufgehen,*** also in $z_1 z_2$ und $\varrho_1 z_2$ ***zugleich,*** mithin vermöge der ***zweiten***

Gleichung (8.), nach (§. 18.), auch in $\varrho_2 z_2$ und folglich in $\varrho_1 z_2$ und $\varrho_2 z_2$ ***zugleich,*** folglich auch vermöge der *dritten* Gleichung (8.), nach (§. 18.), in $\varrho_3 z_2$, und so weiter; folglich zuletzt vermöge der vorletzten der Gleichungen (8.) auch in z_2, und mithin in u und z_2 ***zugleich;*** was wieder der Voraussetzung entgegen ist, so dafs auch hier ein Gemeintheiler λ von u und $z_1 z_2$ nicht gröfser als 1 sein kann.

G. Es können also in *keinem* Fall u und das Product $z_1 z_2$ einen Theiler $\lambda > 1$ gemein haben, insofern u und z_2 einen solchen Gemeintheiler *nicht* haben oder *theilerfremd* sind. Dafs u und z_1 *theilerfremd* sind ist in (***C.***) bedungen worden, weil ohne das nicht nothwendig die vorletzten Reste r_{n-1} und ϱ_{n-1} gleich 1 sein und folglich von den Gleichungen (7. und 8.) die vorletzten nicht Statt finden würden. Also folgt, dafs ***u, in der Voraussetzung,*** es sei sowohl zu z_1 als zu z_2 ***theilerfremd,*** auch nothwendig zu dem Product $z_1 z_2$ von z_1 und z_2 *theilerfremd* sein mufs.

Beweis von II. ***H.*** Eine *untheilbare* Zahl p hat keinen andern Theiler > 1 als *sich selbst.* Sie ist daher zu z_1 und z_2 *immer* theilerfremd, wenn sie nicht etwa selbst in z_1 oder z_2 *aufgeht.* Also folgt aus (I.), dafs die untheilbare Zahl p, wenn sie nicht selbst in z_1 oder in z_2 aufgeht, auch in das Product $z_1 z_2$ von z_1 und z_2 nicht aufgehen kann; wie es (II.) behauptet.

I. Übrigens ändert sich an dem Beweise offenbar nichts, es mögen z_1 und z_2 einander gleich oder ungleich, zu einander theilerverwandt oder theilerfremd sein; dem Lehrsatz gemäfs.

Anm. Der Beweis beruht zunächst auf dem Umstande, dafs zufolge (§. 19.) die Gleichungen (4.) ***nur dann*** nothwendig Statt finden, wenn u und z_1 und z_2 theilerfremd sind; aufserdem auf dem Lehrsatz (§. 18.).

§. 21.

Erläuterung.

Jede theilbare ganze Zahl z kann z. B. durch

$$z = a^\alpha b^\beta c^\gamma d^\delta \ldots . n^\nu$$

ausgedrückt werden, wo die Factoren $a, b, c, d \ldots . n$ von z entweder theilbare, unter einander theilerverwandte, oder theilerfremde, oder auch untheilbare ganze Zahlen sein *können,* die Exponenten $\alpha, \beta, \gamma, \ldots . \nu$ aber *nothwendig* ganze *positive* Zahlen sind.

Denn eine theilbare ganze Zahl z ist nichts anderes als das ***Product*** anderer ganzen Zahlen, die selbst wiederum theilbar, unter einander theilerverwandt, oder theilerfremd, oder auch untheilbar sein können. Diejenigen unter diesen Factoren, welche einander *gleich sind,* wie z. B. alle die, welche gleich a sind, geben für sich, in einander multiplicirt, eine ***Potenz*** mit ganzzahligen positiven Exponenten. Z. B. wenn a αmal als Factor vorkommt, so entsteht daraus die Potenz a^α; b, wenn es β*mal* vorkommt, giebt die Potenz b^β u. s. w., und das Product aller dieser Potenzen macht die Zahl z aus.

§. 22.

Lehrsatz.

I. *Wenn von einer ganzen Zahl* z, *die nach* (§. 21.) *immer durch*

$$1.\quad z = a^\alpha b^\beta c^\gamma d^\delta \ldots\ldots n^\nu$$

ausgedrückt werden kann, keiner der Factoren a, b, c, d, ... n *mit einer andern beliebigen ganzen Zahl* u *theilerverwandt ist, so ist auch* z *selbst mit* u *nicht theilerverwandt, sondern zu* u *theilerfremd.*

II. *Wenn von einer ganzen Zahl*

$$2.\quad z = a^\alpha b^\beta c^\gamma d^\delta \ldots\ldots n^\nu$$

keiner der Factoren a, b, c, d, ... n *mit irgend einem der Factoren* a_1, b_1, c_1, ... k_1 *einer andern ganzen Zahl*

$$3.\quad u = a_1^{\alpha_1} b_1^{\beta_1} c_1^{\gamma_1} \ldots\ldots k_1^{\varkappa_1}$$

theilerverwandt ist, so sind auch z *und* u *selbst nicht theilerverwandt, sondern zu einander theilerfremd.*

III. *Wenn die Factoren* a, b, c, ... n *und* a_1, b_1, c_1, ... k_1 *der beiden Zahlen* z *und* u (2. u. 3.) *sämmtlich Stammzahlen sind, und keiner der Factoren* a, b, c, ... n *ist irgend einem der Factoren* a_1, b_1, c_1, ... k_1 *gleich, so sind* z *und* u *zu einander theilerfremd.*

Beweis von I. *A.* Da nach der Voraussetzung a in (1.) zu u theilerfremd ist, so ist es nach (§. 20. I.) auch das ***Product*** $a.a$ oder a^2. Folglich sind a und a^2 ***beide*** zu u theilerfremd. Also ist es nach (§. 20. I.) auch ihr ***Product*** $a.a^2$ oder a^3. Also sind a und a^3 ***beide*** zu u theilerfremd, und folglich ist es auch ihr ***Product*** $a.a^3 = a^4$. Und so weiter. Also ist zuletzt a^α zu u theilerfremd.

B. Aus gleichen Gründen sind, da *b, c, d, ... n* sämmtlich der Voraussetzung nach zu *u* theilerfremd sind, auch b^β, c^γ, d^δ, ... n^ν zu *u* theilerfremd. U. s. w.

C. Da weiter z. B. a^α und b^β *beide* zu *u* theilerfremd sind, so ist es nach (§. 20. I.) auch ihr ***Product*** $a^\alpha b^\beta$. Und da demzufolge $a^\alpha b^\beta$ und c^γ (*B.*) *beide* zu *u* theilerfremd sind, so ist es nach (§. 20. I.) auch ihr ***Product*** $a^\alpha b^\beta c^\gamma$. So ist weiter, aus gleichen Gründen, $a^\alpha b^\beta c^\gamma d^\delta$ u. s. w. und folglich zuletzt $z = a^\alpha b^\beta c^\gamma d^\delta \ldots . n^\nu$ nothwendig zu *u* theilerfremd; wie es (I.) behauptet.

Beweis von II. *D.* Da nach der Voraussetzung in (II.) keiner der Factoren a_1, b_1, c_1, ... k_1 von *u* z. B. mit dem Factor *a* von *z* theilerverwandt ist, so ist nach (I.) auch *u* selbst mit *a nicht* theilerverwandt. Aus demselben Grunde ist *u* auch mit keinem andern der Factoren von *z* theilerverwandt. Also ist kein Factor von *z* mit *u* theilerverwandt und folglich nach (I.) auch *z* selbst nicht; gemäfs (II.).

Beweis von III. Nur *einander gleiche* Stammzahlen sind theilerverwandt; denn keine Stammzahl hat einen andern Theiler >1, als sich selbst. Nun soll in (III.) keiner der Stammfactoren von *z* irgend einem der Stammfactoren von *u gleich sein:* also ist keiner der Factoren von *z* irgend einem der Factoren von *u* theilerverwandt, und folglich sind nach (II.) *z* und *u* selbst einander *nicht* theilerverwandt, sondern theilerfremd.

Anm. Der Beweis von (I.) beruht auf der wiederholten Anwendung des Lehrsatzes (§. 20. I.). Der Beweis von (II.) beruht auf der Anwendung von (I.) zunächst auf die einzelnen Factoren von *z;* der Beweis von (III.) beruht darauf, dafs hier die Factoren von *u* und *z* von selbst in dem in (II.) vorausgesetzten Falle sind.

§. 23.

Lehrsatz.

Der gröfste Gemeintheiler zweier ganzen Zahlen z *und* u *ist das* ***Product aller derjenigen Stammfactoren****, welche* z *und* u *gemein haben.*

Beispiel. Der gröfste Gemeintheiler von

1. $z = 3^5.7^4.11.13^3.17^2$ und $u = 3^7.7^2.17^3.19^2$

ist

$$2. \quad 3^5 . 7^2 . 17^2 .$$

Nur die Stammfactoren von (2.) kommen in z und u ***zugleich*** vor.

Beweis. ***A.*** Man bezeichne das Product ***aller*** Stammfactoren, welche z und u ***gemein haben,*** durch v, die Producte der ***übrigen*** Stammfactoren in z und in u durch z_1 und u_1, so daſs also

$$3. \quad \frac{z}{u} = \frac{v . z_1}{v . u_1}$$

ist. Hier ist $\frac{v . z_1}{v . u_1}$ nichts anderes als der Bruch $\frac{z_1}{u_1}$ im Zähler und Nenner durch die ***gleiche*** Zahl v multiplicirt. Also ist nach (§. 13. *I.* 8.)

$$4. \quad \frac{z}{u} = \frac{z_1}{u_1} .$$

B. Nach der Voraussetzung sind in v ***alle*** diejenigen Stammfactoren von u enthalten, die zugleich in z vorkommen. Also sind alle Stammfactoren, die u_1 noch sonst enthält, von allen, die noch in z_1 vorkommen, ***verschieden.*** Deshalb sind denn zufolge (§. 22. III.) z_1 und u_1 in (4.) ***theilerfremd;*** das heiſst, sie haben keinen Factor > 1 weiter gemein. Folglich ist v, nemlich das Product ***aller*** Stammfactoren, welche z und u ***gemein haben,*** der ***gröſste*** Gemeintheiler von z und u; wie es der Lehrsatz behauptet.

§. 24.

Lehrsatz.

Wenn eine ganze Zahl z ***mit einer andern ganzen Zahl*** u ***aufgeht, so müssen unter den Stammfactoren von*** z ***nothwendig alle Stammfactoren von*** u ***ohne Ausnahme vorkommen.***

Beweis. ***A.*** Es sei

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots . n^\nu ,$$

wo ***a, b, c, ... n Stammzahlen*** sind. Käme in u irgend ein Stammfactor v vor, der keinem der Stammfactoren $a, b, c, \dots . n$ ***gleich*** wäre, so ginge v in ***keinen*** dieser Factoren auf, also zuerst in a nicht. Deshalb geht denn v nach (§. 20. II.) auch in $a . a = a^2$ nicht auf; folglich auch nicht in $a . a^2 = a^3$ u. s. w., und folglich nicht in a^α. Auch in b geht v nicht auf, folglich aus gleichen Gründen auch in b^β nicht. Eben so nicht in c^γ, d^δ, ... n^ν, also auch gemäſs (§. 20. II.) in $a^\alpha b^\beta$ nicht, und auch nicht in $a^\alpha b^\beta . c^\gamma = a^\alpha b^\beta c^\gamma$ u. s. w., mithin auch in z selbst nicht.

B. Wenn nun aber z mit dem *Factor* v von u nicht aufgeht, so geht auch nach (§. 15. I.) *u selbst* in z nicht auf. Es ist also, wenn u in z aufgeht, nicht möglich, dafs u irgend einen Factor v habe, der von allen Stammfactoren von z verschieden wäre.

§. 25.

Lehrsatz.

I. *Wenn eine ganze Zahl* u *in das* **Product** $z_1 z_2$ *zweier ganzen Zahlen* z_1 *und* z_2 *aufgeht, und sie ist zu einer derselben, z. B. zu* z_1, *theilerfremd, so mufs sie nothwendig in die andere* z_2 *aufgehen.*

II. *Ist dagegen* u *zu keiner der beiden Zahlen* z_1 *und* z_2 *theilerfremd, so kann* u *in das Product* $z_1 z_2$ *aufgehen, obgleich weder in* z_1 *noch in* z_2.

Beispiele. *No. 1.* zu I. $u = 16$ geht in $z_1 z_2 = 75.144 = 10800$ auf und ist zu $z_1 = 75$ *theilerfremd.* Deshalb mufs $u = 16$ in $z_2 = 144$ aufgehen.

No. 2. zu II. $u = 120$ ist weder zu $z_1 = 75$ noch zu $z_2 = 144$ theilerfremd und geht in $z_1 z_2 = 75.144 = 10800$ auf, obgleich weder in 75, noch in 144.

Beweis von I. *A.* Da u in das Product $z_1 z_2$ aufgehen soll, so müssen nach (§. 24.) in diesem Product *alle* Stammfactoren von u ohne Ausnahme vorkommen. Nun sollen z_1 und u *theilerfremd* sein, das heifst, es soll in z_1 *keiner* der Stammfactoren von u vorkommen. Also müssen *alle* Stammfactoren von u ohne Ausnahme in z_2 allein vorhanden sein, und folglich mufs u selbst, welches das Product seiner Stammfactoren ist, nothwendig in z_2 aufgehen.

Beweis von II. *B.* Sind u und z_1 *nicht theilerfremd,* so hat z_1 mit u Stammfactoren gemein; angenommen *nicht alle.* Enthält nun das Product $z_1 z_2$ die verschiedenen Stammfactoren von u zusammen nur gerade *so oft,* als sie in u vorkommen, welches schon hinreicht, damit u in $z_1 z_2$ aufgehe, so enthält z_2 nicht mehr *alle* Stammfactoren von u, indem z_1 schon einige davon wegnimmt. Also geht in diesem Falle nach (§. 24.) u nicht mehr in z_2 auf, eben so wenig wie in z_1, obschon gleichwohl in $z_1 z_2$.

§. 26.

Lehrsatz.

Wenn eine ganze Zahl** z **mit jeder der verschiedenen Zahlen** v_1, v_2, v_3, ... v_n **aufgeht, so geht sie auch mit ihrem Product

$$1. \quad u = v_1 v_2 v_3 \ldots v_n$$

auf, jedoch nothwendig nur dann, wenn keine der Zahlen** v **einen Stammfactor mit der andern gemein hat.

Beispiel 1. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 8, 21 und 25 auf, deren keine einen Stammfactor mit der andern gemein hat. Deshalb geht sie *nothwendig* auch mit ihrem *Product* $8.21.25 = 4200$ auf.

2. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 12, 36 und 105 auf, welche Stammfactoren mit einander gemein haben, nicht aber mit ihrem Product $12.36.105 = 45360$.

Beweis. *A.* Da nach der Voraussetzung z mit v_1, v_2, v_3, ... v_n aufgehen soll, so müssen nach (§. 24.) unter den Stammfactoren von z *alle* Stammfactoren von v_1, v_2, v_3, ... v_n ohne Ausnahme, also *alle* Stammfactoren von u sein.

B. Es geht also nothwendig z eben sowohl z. B. mit v_1 auf, als u. Setzt man daher

$$2. \quad z = v_1 z_1,$$

so ist z_1 eine *ganze* Zahl.

C. Sind nun alle Stammfactoren jedes der Factoren v von denen der übrigen *verschieden*, so wird durch die Division von z durch v_1 *keiner* der Stammfactoren von v_2, v_3, ... v_n weggenommen; mithin enthält z_1 in (2.) noch alle diese letzteren Stammfactoren vollständig.

D. Nun ist zufolge (2.)

$$3. \quad \frac{z}{u} = \frac{v_1 z_1}{v_1 v_2 v_3 \ldots v_n} = \frac{z_1}{v_2 v_3 v_4 \ldots v_n} \quad (\text{§. 13. } I. \ 8.)$$

und es kann z_1, da es noch alle Stammfactoren von v_2, v_3, ... v_n enthält, durch v_2 dividirt werden, so dafs, wenn man

$$4. \quad z_1 = v_2 z_2$$

setzt, z_2 eine *ganze* Zahl ist. Und zwar enthält wieder z_2 noch alle Stammfactoren von v_3, v_4, ... v_n vollständig.

E. Vermöge (3. u. 4) ist weiter

$$5. \quad \frac{z}{u} = \frac{v_2 z_2}{v_2 v_3 v_4 \ldots v_n} = \frac{z_2}{v_3 v_4 \ldots v_n},$$

wo wiederum z_2 mit v_3 aufgeht.

F. Fährt man so fort, so findet sich zuletzt

$$6. \quad \frac{z}{u} = \frac{z_{n-1}}{v_n},$$

wo z_{n-1} noch alle Stammzahlen von v_n enthalten mufs und folglich mit v *aufgeht.*

Also ist $\frac{z}{u}$ nothwendig eine *ganze* Zahl; das heifst, z geht nothwendig mit dem Product $u = v_1 v_2 v_3 \ldots . v_n$ auf; wie es der Lehrsatz behauptet.

G. Sind dagegen nicht alle Stammfactoren jedes v von dem jedes anderen v verschieden, so kann es sein, dafs z. B. schon bei der Division von z durch v_1 in (*B.*) Factoren von z weggenommen werden, die auch noch für ein anderes v, z. B. für v_2 nöthig sind, und folglich sind dann in (4.) *nicht* mehr nothwendig alle Stammfactoren von $v_2, v_3, v_4, \ldots . v_n$ in z_1 enthalten. Mithin geht dann in diesem Fall z_1 schon nicht mehr nothwendig mit v_2 auf, und folglich auch z nicht mit u.

§. 27.

Lehrsatz.

Zwei ganze Zahlen z *und* y *können einander nicht anders gleich sein, als wenn die eine alle die Stammfactoren der andern ohne Ausnahme enthält, und auch keine mehr; so dafs also eine ganze Zahl nur auf eine einzige Art durch die Multiplication aus Stammfactoren zusammengesetzt werden kann.*

Beweis. Wenn $z = y$ sein soll, so mufs y in z und z in y *aufgehen.* Damit y in z *aufgehe*, mufs vermöge (§. 24.) z *alle* Stammfactoren von y enthalten; also keinen *weniger* als y. Und damit z in y aufgehe, mufs y *alle* Stammfactoren von z enthalten; also y keinen *weniger* als z; folglich z keinen *mehr* als y. Es mufs also z alle Stammfactoren von y enthalten, keinen *weniger* und keinen *mehr* als y, und umgekehrt. Folglich kann eine ganze Zahl nur auf eine einzige Weise ein Product von Stammfactoren sein. Andere Stammfactoren geben Zahlen, die nicht mehr in die vorige *aufgehen* und folglich auch nicht ihr gleich sein können.

§. 28.

Lehrsatz.

I. *Eine ganze Zahl ist immer gerade, das heifst, sie geht mit* 2 *auf, wenn entweder nur einer oder wenn mehrere ihrer Factoren gerade*

sind. Die Zahl kann nur dann ungerade sein, das heifst, nicht mit* 2 *aufgehen, wenn kein einziger ihrer Factoren gerade ist. In diesem Falle aber ist* z *nothwendig ungerade.

II. ***Alle Stammzahlen, aufser der einzigen Stammzahl* 2, *sind ungerade Zahlen.***

III. ***Jede gerade Zahl kann durch***

1. $2mn + 0 \pm 2, \pm 4, \pm 6, \ldots \pm m$, ***oder auch***

2. $2mn + 0 \pm 2, \pm 4, \pm 6, \ldots \pm (m-1)$

ausgedrückt werden, wo* n *jede beliebige Zahl und* m *in* (1.) *jede gerade, in* (2.) *jede ungerade Zahl sein kann. In* (1.) *wird durch* $2mn \pm m$ *eine und dieselbe Zahl doppelt ausgedrückt; in* (2.) *nicht.

IV. ***Jede ungerade Zahl, also auch jede Stammzahl* >2, *kann durch***

3. $2mn \pm 1, \pm 3, \pm 5, \ldots \pm (m-1)$, ***oder durch***

4. $2mn \pm 1, \pm 3, \pm 5, \ldots \pm m$

ausgedrückt werden, wo* n *jede beliebige Zahl und* m *in* (3.) *jede gerade, in* (4.) *jede ungerade Zahl sein kann. In* (4.) *wird durch* $2mn \pm m$ *eine und dieselbe Zahl doppelt ausgedrückt; in* (3.) *nicht.

Beweis von I. ***A.*** Wenn einer oder mehrere Factoren der Zahl *z* ***gerade*** sind, also mit 2 aufgehen, so müssen diese Factoren unter ihren ***Stammfactoren*** nothwendig die Stammzahl 2 haben. Also kommt 2 unter den Stammfactoren von *z* ein- oder mehreremale vor. Kommt aber der Stammfactor 2 auch nur einmal vor, so geht *z* mit 2 auf. Also ist die Zahl *z* ***immer*** gerade, sobald nur einer oder auch mehrere ihrer Factoren gerade sind.

B. Ist kein einziger Factor von *z* gerade, das heifst, geht keiner derselben mit 2 auf, so kommt in keinem, und folglich auch in *z* selbst nicht, der Stammfactor 2 vor. Mithin geht dann, und nur dann, *z* mit 2 ***nicht*** auf und ist folglich nothwendig ***ungerade.***

Beweis von II. ***C.*** Eine Stammzahl >2 kann deshalb keine ***gerade*** Zahl sein, weil sie sonst mit 2 aufgehen, folglich einen Theiler >1 haben müfste, und mithin keine Stammzahl sein würde.

Beweis von III. ***D.*** Dafs alle die durch (1. u. 2.) ausgedrückten Zahlen ***gerade*** sind, ist offenbar; denn sie gehen alle mit 2 auf.

Dafs es keine andern ***geraden*** Zahlen weiter gebe, als die, welche durch (1. u. 2.) ausgedrückt werden, läfst sich am kürzesten an ***bestimmten*** Werthen von *m* zeigen.

a. Es sei zuerst für *gerade m,* z. B. $m=6$, also $2m=12$, so werden *alle* gerade Zahlen 0, 2, 4, 6, 8 etc. der Reihe nach wie folgt ausgedrückt:

$$5.\quad \left\{\begin{array}{lllllll} & & & 0.12, & 0.12+2, & 0.12+4, & 0.12+6, \\ 1.12-6, & 1.12-4, & 1.12-2, & 1.12, & 1.12+2, & 1.12+4, & 1.12+6, \\ 2.12-6, & 2.12-4, & 2.12-2, & 2.12, & 2.12+2, & 2.12+4, & 2.12+6, \\ 3.12-6, & 3.12-4, & 3.12-2, & 3.12, & 3.12+2, & 3.12+4, & 3.12+6, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right.$$

Für die erste horizontale Reihe ist $n=0$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m.0+0, 2, 4, 6\ (=m)$ ausgedrückt. Für die zweite horizontale Reihe ist $n=1$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m.1\pm0, \pm2, \pm4, \pm6\,(=m)$ ausgedrückt. Für die dritte horizontale Reihe ist $n=2$; die Zahlen, welche in dieser Zeile stehen, werden durch $2m.2\pm0, \pm2, \pm4, \pm6\,(=m)$ ausgedrückt; u. s. w. Allgemein also drückt, für *irgend ein n,* $2mn\pm0, \pm2, \pm4, \ldots \pm m$ *jede mögliche gerade* Zahl aus. Dabei ist die *letzte* Zahl jeder Reihe *dieselbe,* wie die erste der nächstfolgenden Reihe: also drückt $2mn\pm m$ eine und dieselbe Zahl *doppelt* aus.

b. Es sei für *ungerade m,* z. B. $m=5$, also $2m=10$, so werden *alle* geraden Zahlen 0, 2, 4, 6, 8, etc. der Reihe nach wie folgt ausgedrückt:

$$6.\quad \left\{\begin{array}{lllll} & & 0.10, & 0.10+2, & 0.10+4, \\ 1.10-4, & 1.10-2, & 1.10, & 1.10+2, & 1.10+4, \\ 2.10-4, & 2.10-2, & 2.10, & 2.10+2, & 2.10+4, \\ 3.10-4, & 3.10-2, & 3.10, & 3.10+2, & 3.10+4, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right.$$

Hier ist der Ausdruck der Zahlen in der ersten Zeile $0.10+0, 2, 4\ (=m-1)$, derer in der zweiten Reihe $1.10\pm0, \pm2, \pm4\,(=m-1)$, derer in der dritten Reihe $2.10\pm0, \pm2, \pm4\ (=m-1)$; und so weiter. Allgemein also drückt $2mn\pm0, \pm2, \pm4, \ldots \pm(m-1)$, mit irgend einem Werth von *n,* jede mögliche *gerade* Zahl aus. Dabei aber kommt, in dem gegenwärtigen Fall eines *ungeraden m,* anders wie in (5.) für ein *gerades m, keine* Zahl *zweimal* vor, und *keine* wird also doppelt ausgedrückt.

Dieses ist zusammen, was (III.) behauptet.

E. Auf eine ähnliche Weise läfst sich zeigen, dafs die durch (3. u. 4.) ausgedrückten Zahlen, welche offenbar alle *ungerade* sind, weil keine mit 2 aufgeht, *alle ungleichen ungeraden* Zahlen sind.

a. Es sei zuerst für *gerade m*, z. B. wieder $m = 6$, also $2m = 12$, so werden *alle* ungeraden Zahlen 1, 3, 5, 7, 9, ... der Reihe nach wie folgt ausgedrückt:

$$7.\quad\begin{cases} \qquad\qquad\qquad\qquad\qquad\qquad\quad 0.12+1,\ 0.12+3,\ 0.12+5, \\ 1.12-5,\ 1.12-3,\ 1.12-1,\ 1.12+1,\ 1.12+3,\ 1.12+5, \\ 2.12-5,\ 2.12-3,\ 2.12-1,\ 2.12+1,\ 2.12+3,\ 2.12+5, \\ 3.12-5,\ 3.12-3,\ 3.12-1,\ 3.12+1,\ 3.12+3,\ 3.12+5, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Die Zahlen in der ersten horizontalen Reihe werden durch $0m + 0$, 1, 3, 5 ($= m - 1$) ausgedrückt; also ist für sie $n = 0$. Die Zahlen der zweiten Reihe werden durch $2m.1 \pm 1$, ± 3, ± 5 ($= m - 1$) ausgedrückt; also ist für sie $n = 1$. Die der dritten Reihe werden durch $2m.2 \pm 1$, ± 3, ± 5 ($= m - 1$) ausgedrückt; also ist für sie $n = 2$; und so weiter. Für *irgend einen* Werth von n drückt also $2mn \pm 1$, ± 3, ± 5, ... $\pm(m - 1)$ *jede mögliche* ungerade Zahl aus, und zwar keine zweimal; denn in (7.) ist keine der Zahlen dieselbe.

b. Für *ungerade m* sei wieder $m = 5$, also $2m = 10$, so werden *alle* ungerade Zahlen 1, 3, 5, 7, 9 wie folgt ausgedrückt:

$$8.\quad\begin{cases} \qquad\qquad\qquad\qquad\qquad\qquad\quad 0.10+1,\ 0.10+3,\ 0.10+5, \\ 1.10-5,\ 1.10-3,\ 1.10-1,\ 1.10+1,\ 1.10+3,\ 1.10+5, \\ 2.10-5,\ 2.10-3,\ 2.10-1,\ 2.10+1,\ 2.10+3,\ 2.10+5, \\ 3.10-5,\ 3.10-3,\ 3.10-1,\ 3.10+1,\ 3.10+3,\ 3.10+5, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Die Zahlen der ersten horizontalen Reihe werden durch $2m.0 + 1$, 3, 5 ($= m$) ausgedrückt, und es ist für sie $n = 0$. Die Zahlen der zweiten Zeile werden durch $2m.1 \pm 1$, ± 3, ± 5 ($= m$) ausgedrückt, und es ist für sie $n = 1$. Die Zahlen der dritten Reihe werden durch $2m.2 \pm 1$, ± 3, ± 5 ($= m$) ausgedrückt, und es ist für sie $n = 2$; u. s. w. Also drückt allgemein $2mn \pm 1$, ± 3, ± 5, ... $\pm m$ für *irgend ein n jede mögliche* ungerade Zahl aus; und zwar je die letzte in den verschiedenen Reihen *zweimal*, denn je die erste in den nächstfolgenden Reihe sind dieselben.

Dieses ist zusammen was (IV.) behauptet.

Anm. *F.* Für die *ungeraden Stammzahlen* setzt man am gewöhnlichsten $m = 2$ und drückt sie also nach (3.) durch

$$9.\quad 4n \pm 1$$

aus; denn mehrere Eigenschaften der durch $4n + 1$ bezeichneten Stammzahlen sind, wie sich weiter unten ergeben wird, von denen der Stammzahlen $4n - 1$ wesentlich verschieden.

§. 29.

Lehrsatz.

Es werde die beliebige ganze Zahl z *durch ihre Stammfactoren* a, b, c, d, ... n *ausgedrückt, nemlich nach* (§. 21.) *durch*

$$1.\quad z = a^{\alpha} b^{\beta} c^{\gamma} d^{\delta} \dots n^{\nu},$$

wo $\alpha, \beta, \gamma, \delta, \dots \nu$ *ganze positive Zahlen sind. Alsdann geht*

I. ***Jedes Glied der Reihe, welche das Product***

$$2.\quad P = (1+a+a^2 \dots + a^{\alpha})(1+b+b^2 \dots + b^{\beta})(1+c+c^2 \dots + c^{\gamma}) \dots \dots (1+n+n^2 \dots + n^{\nu})$$

entwickelt giebt, in z *auf. Auch hat* z ***keine andern*** *Theiler aufser diesen Gliedern.*

II. *Die* ***Anzahl*** *der Theiler von* z *ist, die Einheit und* z *mit eingeschlossen,*

$$3.\quad \tau = (\alpha+1)(\beta+1)(\gamma+1) \dots (\nu+1).$$

III. *Ist* τ (3.) *eine gerade Zahl, so sind* $\frac{1}{2}\tau$ *Theiler von* z ***kleiner*** *und* $\frac{1}{2}\tau$ *Theiler* ***gröfser*** *als die* ***Quadratwurzel*** *aus* z. *Ist* τ ***ungerade,*** *so sind* $\frac{1}{2}(\tau-1)$ *Theiler von* z ***kleiner*** *und* $\frac{1}{2}(\tau-1)$ *Theiler* ***gröfser*** *als die Quadratwurzel von* z. *Die Zahl* z *ist in diesem Falle eine* ***Quadratzahl;*** *alle die Zeiger* $\alpha, \beta, \gamma, \dots \nu$ *sind dann nothwendig* ***gerade,*** *und der eine noch übrige Theiler von* z, *der durch*

$$4.\quad \sqrt{z} = a^{\frac{1}{2}\alpha} b^{\frac{1}{2}\beta} c^{\frac{1}{2}\gamma} \dots n^{\frac{1}{2}\nu}$$

ausgedrückt wird, ist die ***Quadratwurzel*** *von* z.

IV. *Die* ***Summe*** *aller Theiler von* z *ist*

$$5.\quad s = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \dots \frac{n^{\nu+1}-1}{n-1}.$$

Beispiel 1. Es sei

$$6.\quad z = 2^3.3^2.5 = 360,$$

also

$$7.\quad a=2,\quad b=3,\quad c=5,\quad \alpha=3,\quad \beta=2,\quad \gamma=1.$$

Alsdann ist nach (1.)

$$8.\quad P = (1+2+4+8)(1+3+9)(1+5),$$

und dieses giebt, entwickelt:

$$9.\quad P = 1+2+4+8+3+6+12+24+9+18+36+72+5+10+20 +40+15+30+60+120+45+90+180+360.$$

Jedes Glied dieses entwickelten Products geht in $z=360$ auf und es giebt

keinen andern Theiler von z aufser diesen Gliedern. Die Anzahl τ der Theiler ist 24, und (3.) giebt, wie gehörig,

$$10. \quad \tau = (3+1)(2+1)(1+1) = 4.3.2 = 24.$$

τ ist hier also ***gerade.*** Die $\frac{1}{2}\tau = 12$ Theiler 1, 2, 4, 8, 3, 6, 12, 9, 18, 5, 10, 15 sind ***kleiner*** als die Quadratwurzel von z, welche zwischen 18 und 19 liegt; die übrigen $\frac{1}{2}\tau = 12$ Theiler sind ***gröfser*** als $\sqrt{z}$. Die ***Summe*** s der Theiler beträgt 1170, und wie gehörig giebt (5.)

$$11. \quad s = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{15}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 15.13.6 = 1170.$$

2. Es sei

$$12. \quad z = 2^4.3^2 = 144,$$

so dafs

$$13. \quad a = 2, \quad b = 3, \quad \alpha = 4, \quad \beta = 2$$

ist, so ist in (1.)

$$14. \quad P = (1+2+4+8+16)(1+3+9),$$

und dieses giebt, entwickelt:

$$15. \quad P = 1+2+4+8+16+3+6+12+24+48+9+18+36+72+144.$$

Alle Glieder dieses entwickelten Products sind aufgehende Theiler von $z = 144$, und es giebt keine andern. Die Anzahl τ dieser Theiler ist 15, und (3.) giebt, wie gehörig,

$$16. \quad \tau = (4+1)(2+1) = 5.3 = 15.$$

τ ist ***hier ungerade.*** Die $\frac{1}{2}(\tau-1) = 7$ Theiler, 1, 2, 4, 8, 3, 6, 9 sind kleiner als die Quadratwurzel von z, welche 12 ist; die $\frac{1}{2}(\tau-1) = 7$ Theiler 16, 24, 48, 18, 36, 72 und 144 sind ***gröfser*** als die Quadratwurzel aus z. Der letzte, 15te Theiler ist 12, nemlich

$$17. \quad \sqrt{z} = 2^{\frac{4}{2}}.3^{\frac{2}{2}} = 2^2.3 = 4.3 = 12.$$

z ist hier eine ***Quadratzahl.*** Die ***Summe*** der Theiler ist 403, und wie gehörig giebt (5.)

$$18. \quad s = \frac{2^5-1}{2-1} \cdot \frac{3^3-1}{3-1} = \frac{31}{1} \cdot \frac{26}{2} = 31.13 = 403.$$

Beweis von I. ***A.*** z kann nicht mit ***andern*** Stammzahlen als a, b, c, d, ... n aufgehen (§. 14. II. u. §. 24.). Es geht aber nach (§. 14. I.) mit a, b, c, ... n und mit allen ***Potenzen*** von a, b, c, ... n auf, deren Zeiger nicht höher sind als α, β, γ, ... ν, und mit keinen andern; so wie mit allen ***Producten*** dieser Potenzen; denn alle diese sind ***Factoren*** von z. Es kommt daher nur darauf an, die verschiedenen möglichen Producte jener Potenzen zu finden.

B. Wäre zuerst blofs

$$19. \quad z = a^\alpha b^\beta,$$

so wären die sämmtlichen möglichen Theiler von z die Potenzen $a^0 = 1$, a^1, a^2, a^3, ... a^α von a, und $b^0 = 1$, b^1, b^2, b^3, ... b^β von b, nebst allen möglichen Producten derselben. Man findet dieselben *alle*, nemlich die ***Producte*** und die ***Potenzen selbst***, wenn man $1 + a + a^2 \ldots + a^\alpha$ mit $1 + b + b^2 \ldots \ldots + b^\beta$ ***multiplicirt.*** Denn zuerst 1mal $1 + a + a^2 \ldots + a^\alpha$ giebt alle Potenzen von a, welche vorkommen können. Darauf bmal $1 + a + a^2 \ldots + a^\alpha$ giebt alle möglichen Producte jener Potenzen mit b, so wie b selbst. b^2mal $1 + a + a^2 \ldots \ldots + a^\alpha$ giebt alle möglichen Producte der vorkommenden Potenzen von a mit b^2, so wie b^2 selbst. Und so weiter. Die Multiplication von $1 + a + a^2 \ldots + a^\alpha$ mit $1 + b + b^2 \ldots + b^\beta$ giebt also alle möglichen Producte der hier vorkommenden Potenzen von a, mit allen vorkommenden Potenzen von b, und zugleich die Potenzenvon a und b selbst; also ***Alles***, was gesucht wird. Mithin sind die verschiedenen Glieder des Productes $(1 + a + a^2 \ldots + a^\alpha)(1 + b + b^2 \ldots + b^\beta)$ sämmtlich Theiler von $z = a^\alpha b^\beta$ (19.) und es giebt keine anderen.

C. Es sei ferner

$$20. \quad z = a^\alpha b^\beta c^\gamma,$$

so gehen offenbar in z zunächst alle Theiler von $a^\alpha b^\beta$ auf, und keine anderen mit nur a oder b zu Stammfactoren. Sie gehen aber alle auch dann noch in z (20.) auf, wenn man sie noch mit c, mit c^2, mit c^3 u. s. w. bis c^γ multiplicirt; jedoch nicht mehr, wenn sie mit einer höheren Potenz von c als c^γ multiplicirt werden. Also findet man die sämmtlichen Theiler von z (20.), wenn man diejenigen von z (19.) mit 1, c, c^2, ... c^γ multiplicirt. Die sämmtlichen Theiler von z (19.) waren die Glieder des Products $(1 + a + a^2 \ldots + a^\alpha)$ $(1 + b + b^2 \ldots + b^\beta)$ (*B.*), also sind die Glieder des Products $(1 + a + a^2 \ldots + a^\alpha)$ $(1 + b + b^2 \ldots + b^\beta)(1 + c + c^2 \ldots + c^\gamma)$ sämmtliche Theiler von z (20.), und es giebt keine andern; denn es können keine höheren Potenzen von c vorkommen als c^γ; die Theiler 1, c, c^2, ... c^γ selbst aber, mit welchen z ebenfalls aufgeht, finden sich in dem Product durch das Glied 1, welches in $(1 + a + a^2 \ldots + a^\alpha)(1 + b + b^2 \ldots + b^\beta)$ vorkommt, ebenfalls.

D. Ganz auf ähnliche Weise folgt, dafs man, im Fall

$$21. \quad z = a^\alpha b^\beta c^\gamma d^\delta$$

ist, alle möglichen Theiler von z findet, wenn man der Reihe nach alle Theiler von z (20.) mit 1, d, d^2, ... d^δ multiplicirt, folglich, da jene Theiler nach (*C.*) die Glieder des Products $(1 + a + a^2 \ldots + a^\alpha)(1 + b + b^2 \ldots + b^\beta)$

$(1+c+c^2\ldots.+c^\gamma)$ sind, wenn man dieses Product noch mit $1+d+d^2\ldots.+d^\delta$ multiplicirt; und so weiter; so dafs also zuletzt die Glieder des Products P (2.) alle möglichen Theiler von z (1.) sind; wie es (I.) behauptet.

Beweis von II. *E.* Die *Anzahl* der Glieder des ersten Factors $1+a+a^2\ldots.+a^\alpha$ von P (2.) ist $\alpha+1$. Multiplicirt man diese Glieder mit den $\beta+1$ Gliedern des zweiten Factors $1+b+b^2\ldots.+b^\beta$, so liefert *jedes* Glied dieses zweiten Factors $\alpha+1$ Producte, also giebt die Multiplication der beiden Factoren überhaupt $(\alpha+1)(\beta+1)$ Glieder; und zwar sind alle diese Glieder unter sich *verschieden.* Denn die ersten unter sich verschiedenen $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2\ldots.+a^\alpha$ mit 1 entstehen, enthalten *kein b;* die zweiten $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2\ldots.+a^\alpha$ mit b entstehen, enthalten *sämmtlich b,* aber keine *höhere* Potenz von *b;* die dritten $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2\ldots.+a^\alpha$ mit b^2 entstehen, enthalten *sämmtlich* b^2, und keine *höhere* Potenz von b u. s. w. Also sind die $(\alpha+1)(\beta+1)$ Glieder sämmtlich von einander *verschieden.*

F. Multiplicirt man weiter die sämmtlichen $(\alpha+1)(\beta+1)$ Glieder, welche das Product $(1+a+a^2\ldots.+a^\alpha)(1+b+b^2+\ldots.+b^\beta)$ enthält, und welche sämmtlich Theiler von z sind, mit den $\gamma+1$ Gliedern von $1+c+c^2\ldots$ $\ldots+c^\gamma$, so entstehen, da jedes dieser Glieder $(\alpha+1)(\beta+1)$ Glieder liefert, zusammen $(\alpha+1)(\beta+1)(\gamma+1)$ Glieder, die alle wieder von einander *verschieden* sind, weil die ersten unter sich verschiedenen $(\alpha+1)(\beta+1)$ Glieder gar kein *c,* die zweiten $(\alpha+1)(\beta+1)$ von c herkommenden Glieder sämmtlich c als Factor, die dritten $(\alpha+1)(\beta+1)$ von c^2 herkommenden Glieder sämmtlich c^2 als Factor enthalten, u. s. w.

So folgt dann, wenn man weiter mit der Multiplication der Factoren von P (2.) fortfährt, dafs die *Anzahl* der Glieder dieses Products gemäfs (3.) $\tau=(\alpha+1)(\beta+1)(\gamma+1)\ldots.(\nu+1)$ ist; und alle diese Glieder sind von einander verschieden. Das ist was (II.) behauptet

Beweis von III. *G.* Da z (1.) mit allen Gliedern des Products P (2.) aufgeht, so ist, wenn z_1 *irgend eines* dieser Glieder und z_2 den *Quotienten* von z dividirt durch z_1 bezeichnet,

$$22.\quad z=z_1 z_2,$$

wo z_2 eine *ganze* Zahl ist. Hieraus folgt, dafs auch der Quotient z_2 in z aufgehen und folglich nothwendig *ebenfalls eins* von den Gliedern des Products P sein mufs. Zu *jedem* Gliede des Products P gehört also nothwendig *ein*

zweites, welches, mit ihm multiplicirt, z giebt. Aber die Glieder des Products P sind *alle* unter sich verschieden (*F*.): also können in (22.) z_1 und z_2 einander *nicht gleich* sein, es wäre denn, dafs z_1 mit *sich selbst* multiplicirt z gäbe und also z eine *Quadratzahl* wäre.

Ist dies nicht der Fall, so ist nothwendig z_1 entweder *kleiner* oder *gröfser* als $\sqrt{z}$. Zu jedem $z_1 < \sqrt{z}$ gehört aber, wegen $z_1 z_2 = z$ (22.), ein $z_2 > \sqrt{z}$. Also giebt es in solchem Falle *gerade eben so viele* Glieder $< \sqrt{z}$ als Glieder $> \sqrt{z}$, und folglich von jeder Art $\frac{1}{2}\tau$.

Ist dagegen *ein* Glied vorhanden, welches, mit sich selbst multiplicirt, z giebt, so bleiben noch $\tau - 1$ Glieder *übrig*, und diese sind dann alle, entweder $< \sqrt{z}$ oder $> \sqrt{z}$. Von *diesen* $\tau - 1$ Gliedern gilt wieder dasselbe wie vorhin; und folglich sind ihrer $\frac{1}{2}(\tau - 1)$ *kleiner* und $\frac{1}{2}(\tau - 1)$ *gröfser* als $\sqrt{z}$. Das übrig bleibende *eine* Glied ist $= \sqrt{z}$.

H. Aber die Zahl τ der Glieder selbst *entscheidet*, ob ein z_1 statt finden könne, welches, *mit sich selbst* multiplicirt, z giebt. Ist nemlich τ *gerade*, so ist $\frac{1}{2}\tau$ eine *ganze* Zahl und folglich bleibt, da nach (*G*.) $\frac{1}{2}\tau$ Glieder kleiner und $\frac{1}{2}\tau$ Glieder gröfser als $\sqrt{z}$ sein müssen, *kein* Glied *übrig*, welches *gleich* $\sqrt{z}$ sein könnte. Die Zahl τ (3.) ist aber nach (§. 28. I.) *immer gerade*, wenn auch nur ein einziger ihrer Factoren $\alpha + 1$, $\beta + 1$, $\gamma + 1$, ... $\nu + 1$ *gerade*, also nur ein einziger der Exponenten α, β, γ, ... ν *ungerade* ist. In solchem Falle also giebt es keine Quadratwurzel aus z, die eine ganze Zahl wäre.

Ist dagegen τ *ungerade*, so ist $\frac{1}{2}(\tau - 1)$ eine *ganze* Zahl, und da alsdann $\frac{1}{2}(\tau - 1)$ Glieder *kleiner* und $\frac{1}{2}(\tau - 1)$ Glieder *gröfser* als $\sqrt{z}$ sind (*G*.), so bleibt *ein Glied* übrig, welches, mit sich selbst multiplicirt, z giebt. Es ist aber τ nach (§. 28. I.) nur dann *ungerade*, wenn *keiner* der Factoren $\alpha + 1$, $\beta + 1$, $\gamma + 1$, ... $\nu + 1$ *gerade*, also wenn *keiner* der Exponenten α, β, γ, ... ν *ungerade* ist. Also *nur* in diesem Fall giebt es eine ganzzahlige Quadratwurzel von z. Dieses zusammen ist was (III.) behauptet.

Beweis von IV. *I.* Die Summe der sämmtlichen Glieder des entwickelten Products P (2.) ist der *Werth* des Products selbst. Nun ist

$$23. \quad 1 + a + a^2 + a^3 \ldots. + a^\alpha = \frac{a^{\alpha+1} - 1}{a - 1};$$

denn multiplicirt man hier rechts und links mit $a - 1$, so ergiebt sich

$$24. \quad \begin{cases} a + a^2 + a^3 + a^4 \ldots. + a^\alpha + a^{\alpha+1} = a^{\alpha+1} - 1, \\ -1 - a - a^2 - a^3 - a^4 \ldots. - a^\alpha \end{cases}$$

wie gehörig. Eben so ist $1+b+b^2 \dots\dots + b^\beta = \frac{b^{\beta+1}-1}{b-1}$, $1+c+c^2 \dots\dots c^\gamma = \frac{c^{\gamma+1}-1}{c-1}$, u. s. w. Also läfst sich P, dessen *Werth* in (5.) durch s bezeichnet wurde, wie folgt ausdrücken:

$$25. \quad s = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \dots\dots \frac{n^{\nu+1}-1}{n-1};$$

wie (IV.) es behauptet.

Anm. Die Hauptmomente in dem Beweise sind, dafs der Ausdruck (1) von z mit keinen *höheren* Potenzen von $a, b, c, \dots\dots n$ aufgeht, als mit denen, deren Exponenten α, β, γ, ... ν sind; sodann, dafs alle diese Potenzen in den Gliedern des Products P (2.) vorkommen; und endlich, dafs alle Glieder des Products P von einander *verschieden* sind.

§. 30.

Lehrsatz.

Jede Menge von Einheiten, also jede ganze Zahl z, *kann, wenn* a *eine beliebige andere, kleinere Menge von Einheiten bezeichnet, durch*

$$1. \quad z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} \dots\dots + x_1 a + x_0$$

ausgedrückt werden, wo die x *sämmtlich ganze Zahlen und sämmtlich kleiner als* a *sind.* m *ist ebenfalls eine ganze Zahl, deren Gröfse sich nach* z *und* a *richtet. Die* x *können für ein- und dasselbe* z *und* a *jedes nur einen Werth haben. Bestimmt man für die verschiedenen Werthe, welche die* x *haben können, und deren* a — 1 *sind, ausschliefsliche, willkürliche Zeichen, und dann noch für Null ebenfalls ein Zeichen, so kann* z *durch diese Zeichen, blofs der Reihe nach hinter einander geschrieben, ausgedrückt werden, ohne* a *selbst zu schreiben. Dieses Mittel Mengen von Einheiten auszudrücken, giebt die Zahlensysteme. Die Zeichen für die verschiedenen möglichen Werthe von* x *sind die Ziffern, und die verschiedenen Potenzen von* a *werden als eben so viele verschiedene Einheiten betrachtet, deren Werthe die Stellen der Ziffern schon ausdrücken. In dem üblichen dekadischen Zahlensystem enthält* a *zehn Einheiten, und die* a — 1 *Ziffern* 1, 2, 3, 4, 5, 6, 7, 8 und 9, *nebst dem Zeichen* 0 *für Null, reichen hin, jede Menge z von Einheiten, also jede ganze Zahl auszudrücken.*

Beweis. *A.* Welche Menge von Einheiten auch z enthalten mag: es wird immer durch wiederholte Multiplication von a mit sich selbst, sobald

a mehr als *eine* Einheit enthält, zu einer Zahl a^m zu gelangen sein, die, wenn man sie *noch einmal* mit a multiplicirt, eine Zahl giebt, welche *gröfser* ist als z. Denn durch wiederholte Multiplication mit a kann man die Menge der Einheiten in dem Product bis *in's Unendliche* vergröfsern.

B. Ist nun a^m diejenige Potenz von a, welche noch *kleiner* als z ist, aber, noch einmal mit a multiplicirt, eine Zahl giebt, die *gröfser* ist als z, so wird sich z durch

$$2.\quad z = x_m a^m + r_1$$

ausdrücken lassen, wo $x_m < a$ und $r_1 < a^m$ ist. Denn wäre x_m gleich a oder $> a$, so wäre $x_m a^m + r_1$ gleich $a^{m+1} + r_1$, also *gröfser* als z, gegen die Voraussetzung; r_1 aber kann immer $< a^m$ gemacht werden, da man nur a^m so oft von z abziehen darf, als es möglich ist.

C. Da also $r_1 < a^m$ ist, aber möglicherweise $> a^{m-1}$ sein kann, so wird sich aus gleichen Gründen r_1 wieder wie folgt ausdrücken lassen:

$$3.\quad r_1 = x_{m-1} a^{m-1} + r_2,$$

wo wieder x_{m-1} nothwendig $< a$ und $r_2 < a^{m-1}$ ist. Eben so wird weiter

$$4.\quad \begin{cases} r_2 = x_{m-2} a^{m-2} + r_3, \\ r_3 = x_{m-3} a^{m-3} + r_4, \\ \ldots\ldots\ldots \end{cases}$$

gesetzt werden können, bis man zuletzt auf ein r kommt, welches kleiner als a selbst ist und folglich in die Reihe der x gehört, die *alle* $< a$ sind.

D. Substituirt man die Ausdrücke (2., 3. u. 4.) in einander, so ergiebt sich der Reihe nach

$$5.\quad \begin{cases} z = x_m a^m + r_1, \\ z = x_m a^m + x_{m-1} a^{m-1} + r_2, \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + r_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} \ldots + x_1 a + x_0. \end{cases}$$

Der letzte dieser Ausdrücke von z ist der (1.) des Lehrsatzes.

E. Bestimmt man nun für die $a-1$ verschiedenen Werthe, welche x haben kann, eben so viele ausschliefsliche, verschiedene Zeichen oder *Ziffern,* z. B. für das dekadische System die Ziffern 1, 2, 3, 4, 5, 6, 7, 8, und 9 und für Null das Zeichen 0, so kann zunächst *a selbst* blofs durch 10 bezeichnet werden; denn für $z = a$ sind in (1.) *alle x,* mit Ausnahme von x_1, gleich Null; x_1 aber ist $= 1$. Also ist z oder $x_1 a + x_0$ hier $1.x + 0.1$, und wenn man nun x selbst als eine neue Einheit betrachtet, welche zehn

der einfachen Einheiten enthält, so kann man blofs schreiben $1.1 + 0.1$, oder zusammengezogen 10, wo schon die ***Stelle*** der 1 ausdrückt, dafs die ***nächst höhere*** Einheit gemeint sei.

Eben so sind für $z = a^2$ ***alle*** x, mit Ausnahme von x_2, gleich Null, und x_2 ist $= 1$. Also ist $z = x_{m-1}a^2 + 0.1 + 0 = 1.1 + 0.1 + 0$, wofür zusammengezogen blofs 100 geschrieben werden kann, da die Stelle der 1 schon anzeigt, welche Potenz von a gemeint sei. Und so weiter.

Sind nun die verschiedenen x ***nicht*** Null, so multipliciren sie der Reihe nach die verschiedenen Einheiten oder Potenzen von a, deren Exponenten schon von den Stellen der Ziffern angezeigt werden; denn keine Ziffer, da sie nur ein einziges Zeichen ist, nimmt mehr als eine Stelle ein.

Also läfst sich jede Menge z von Einheiten blofs durch die hinter einander geschriebenen Ziffern oder Mengen der verschiedenen Potenzen von a ausdrücken.

F. Um zu zeigen, dafs für ein- und dasselbe z und a, die x jedes ***nur einen*** Werth haben können, setze man, es könne ein- und dasselbe z, aufser wie in (1.), auch durch

6. $$z = y_m a^m + y_{m-1} a^{m-1} + y_{m-2} a^{m-2} \ldots\ldots + y_1 a + y_0$$

ausgedrückt werden, wo die y von den x in (1.) ***verschieden*** sind.

Man ziehe (6.) von (1.) ab, so ergiebt sich

7. $$0 = (x_m - y_m) a^m + (x_{m-1} - y_{m-1}) a^{m-1} + (x_{m-2} - y_{m-2}) a^{m-2} \ldots\ldots$$
$$\ldots\ldots + (x_1 - y_1) a^1 + x_0 - y_0.$$

In diesem Ausdruck geht rechterhand Alles bis auf $x_0 - y_0$ mit a auf, also mufs nach (§. 18.) auch $x_0 - y_0$ mit a aufgehen. Dies aber ist nicht anders möglich, als wenn $x_0 - y_0$ gleich ***Null*** ist, da x_0 und y^0 beide nach der Voraussetzung $< a$ sind und also auch $x_0 - y_0 < a$ ist. Also mufs nothwendig y_0 ***gleich*** x_0 sein.

Läfst man $x_0 - y_0$, als Null, aus (7.) weg und dividirt was übrig bleibt durch a, so ergiebt sich

8. $$0 = (x_m - y_m) a^{m-1} + (x_{m-1} - y_{m-1}) a^{m-2} + (x_{m-2} - y_{m-2}) a^{m-3} \ldots\ldots$$
$$\ldots\ldots + (x_2 - y_2) a_2 + x_1 - y_1,$$

und hieraus folgt, ganz aus demselben Grunde wie vorhin, dafs auch y_1 ***gleich*** x_1 sein mufs.

Läfst man wieder $x_1 - y_1$, als Null, aus (8.) weg und dividirt was übrig bleibt durch a, so folgt ferner, dafs auch y_2 ***gleich*** x_2 sein mufs. Und so weiter für alle x und y bis zu $y_m = x_m$ selbst. Also können für ein- und dasselbe z und a die x in (1.) jedes ***nur einen*** Werth haben.

§. 31.

Lehrsatz.

I. ***Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl 2; und zwar nur auf eine Art.***

II. ***Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl 3, weniger der Summe dieser oder jener Potenzen derselben Zahl 3; und zwar wieder nur auf eine Art.***

Beispiel zu I. Es ist $83 = 64 + 16 + 2 + 1 = 2^6 + 2^4 + 2^1 + 2^0$; $74 = 64 + 8 + 2 = 2^6 + 2^3 + 2^1$; $181 = 128 + 32 + 16 + 4 + 1 = 2^7 + 2^5 + 2^4 + 2^2 + 2^0$ u. s. w.

Zu II. Es ist $83 = 81 + 3 - 1 = 3^4 + 3^1 - 3^0$; $74 = 81 - 9 + 3 - 1 = 3^4 - 3^2 + 3^1 - 3^0$; $181 = 243 - 81 + 27 - 9 + 1 = 3^5 - 3^4 + 3^3 - 3^2 + 3^0$.

Beweis von I. *A.* Nach (§. 30.) kann *jede* ganze Zahl durch

1. $z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} \dots + x_1 a + x_0$

ausgedrückt werden, wo a *willkürlich* ist und *alle* $x < a$ sind.

Setzt man also das *willkürliche* $a = 2$, so können die x nur 1 oder 0 sein. Also wird jede Zahl z durch

2. $z = x_m 2^m + x_{m-1} 2^{m-1} + x_{m-2} 2^{m-2} \dots x_1 2 + x_0$

ausgedrückt, wo die x *nie gröfser* als 1, jedoch diese oder jene x auch Null sein können. Also wird jedes z blofs durch *einmal* genommene Potenzen von $a = 2$ ausgedrückt, unter welchen diese oder jene *fehlen* können. Jedes z ist also die Summe dieser oder jener Potenzen (nemlich derer, die *nicht* fehlen) von der Zahl $a = 2$.

B. Ferner können für ein- und dasselbe z und a die x (2.) nach (§. 30.) jedes *nur einen* Werth haben: also kann auch hier z *nur auf eine Art* aus diesen oder jenen Potenzen von 2 zusammengesetzt werden.

Beweis von II. *C.* Setzt man in (1.) $a = 3$, so können die x, weil sie $< a$ sein sollen, nur 0, 1 oder 2 sein. Diejenigen, welche 0 oder 1 sind, geben die Potenzen von $a = 3$ entweder gar nicht, oder blofs einmal. Für diejenigen, welche 2 sein müssen, setze man $2 = 3 - 1 = a - 1$. Dadurch geht das Glied, welches 2 zum Coëfficienten hat, mit einem seiner Theile in die nächst höhere Potenz von a, also zu dem nächstvorhandenen Gliede über, der andere Theil aber kommt dann nur einfach, und zwar negativ vor. Z. B. wenn zwei aufeinander folgende Glieder in (1.) $x_k 3^k + 2.3^{k-1}$ wären, so verwandeln sie sich, wenn man $3 - 1$ statt 2 schreibt, in

$x_k . 3^k + 3 . 3^{k-1} - 3^{k-1} = x_k . 3^k + 3^k - 3^{k-1} = (x_k + 1) 3^k - 3^{k-1}$. Ist hier x_k nicht 0, sondern 1, so bekommt 3^k zum Coëfficienten 2 und man kann wie vorhin verfahren. Ist x_k schon 2, so kann man zuvor schon statt dessen 3 — 1 statt 2 setzen, u. s. w., falls es nöthig ist, bis zum *ersten* Gliede $x_m a^m$ hinauf, welches, wenn $x_m = 2$ wäre, $3 . a^m - a^m = a^{m+1} - a^m$ geben würde. Also lassen sich überall die Coëfficienten 2, wo sie vorkommen, wegschaffen, und es lassen sich die x blofs auf $+1$, -1 und 0 reduciren, also so, dafs z blofs durch eine Summe dieser oder jener Potenzen der Zahl 3, *weniger* der Summe dieser oder jener andern Potenzen derselben Zahl 3 ausgedrückt wird.

D. Dafs solches *nur auf eine Art* geschehen kann, folgt daraus, dafs in (2.) die x nach (§. 30.) allgemein für ein- und dasselbe a und z jedes *nur einen Werth* haben können.

§. 32.

Lehrsatz.

Wenn man eine beliebige gegebene ganze Zahl Z *nach* (§. 30. 1.) *durch*

$$1. \quad Z = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \ldots + x_2 A^2 + x_1 A + x_0$$

ausdrückt, und man setzt

$$2. \quad nA = \mathfrak{G} s + r,$$

wo s *ebenfalls gegeben,* n *willkürlich aber zu* s *theilerfremd und* $r < s$ *ist, so geht* Z (1.) *mit der Zahl* s *auf, oder nicht auf, je nachdem*

$$3. \quad z = x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} + n^3 x_{m-3} r^{m-3} \ldots$$
$$\ldots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0$$

mit s *aufgeht, oder nicht aufgeht.*

Beweis. *A.* Wenn man von (2.) z. B. die kte Potenz nimmt, so ist nach (§. 11. No. 5.)

$$4. \quad n^k A^k = \mathfrak{G} s + r^k;$$

also der Reihe nach

$$5. \quad \begin{cases} nA = \mathfrak{G} s + r, \\ n^2 A^2 = \mathfrak{G} s + r^2, \\ n^3 A^3 = \mathfrak{G} s + r^3, \\ n^4 A^4 = \mathfrak{G} s + r^4, \\ \ldots\ldots\ldots\ldots \\ n^m A^m = \mathfrak{G} s + r^m. \end{cases}$$

B. Nun multiplicire man (1.) mit n^m, so ergiebt sich

$$6.\quad n^m Z = x_m n^m A^m + x_{m-1} n^m A^{m-1} + x_{m-2} n^m A^{m-2} \ldots\ldots + x_2 n^m A^2 + x_1 n^m A + x_0 n^m.$$

Setzt man hierin die Ausdrücke von nA, n^2A^2, n^3A^3, ..., so erhält man

$$\begin{aligned} 7.\quad n^m Z = {} & x_m\ (\mathfrak{S}s + r^m) \\ & + x_{m-1}(\mathfrak{S}s + r^{m-1})n \\ & + x_{m-2}(\mathfrak{S}s + r^{m-2})n^2 \\ & + x_{m-3}(\mathfrak{S}s + r^{m-3})n^3 \\ & \ldots\ldots\ldots\ldots \\ & + x_2\ (\mathfrak{S}s + r^2)\ n^{m-2} \\ & + x_1\ (\mathfrak{S}s + r)\ n^{m-1} \\ & + x_0\ .\ n^m, \end{aligned}$$

oder, nach (§. 11.),

$$8.\quad n^m Z = \mathfrak{S}s + x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} \ldots\ldots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0,$$

oder auch, durch (3.) ausgedrückt,

$$9.\quad n^m Z = \mathfrak{S}s + z.$$

C. Geht nun hier z mit s auf, so gehen die *beiden* Glieder $\mathfrak{S}s$ und z mit s auf. Also mufs alsdann nach (§. 18.) auch das *dritte* Glied $n^m.Z$ mit s aufgehen. Aber n ist nach der Voraussetzung zu s *theilerfremd,* also auch n^m. Mithin geht von den beiden Factoren n^m und Z der Factor n^m *nicht* mit s auf. Dieserhalb mufs zufolge (§. 25. I.) nothwendig der *andere* Factor Z mit s aufgehen. Also folgt, dafs, wenn z (3.) mit s *aufgeht,* auch Z (1.) mit s *aufgehen* mufs.

D. Geht in (9.) z *nicht* mit s auf, so kann auch Z nicht mit s aufgehen, denn sonst wäre $\frac{n^m Z}{s}$, so wie $\frac{\mathfrak{S}s}{s} = \mathfrak{S}$, eine ganze Zahl, also auch in $\frac{n^m Z - \mathfrak{S}s}{s} = \frac{z}{s}$, $\frac{n^m Z - \mathfrak{S}s}{s}$ eine ganze Zahl, $\frac{z}{s}$ dagegen ein Bruch, und einer ganzen Zahl kann ein Bruch nicht gleich sein

Dieses zusammen ist was der Lehrsatz behauptet.

Anm. Der Beweis beruht auf (§. 11, 18. und 25. I.).

§. 33.

Aufgabe.

Ob eine gegebene ganze Zahl Z mit einer andern gegebenen Zahl s *aufgehe,* vermittels anderer, von Z und s abhängender Zahlen z zu finden,

die, während sie ***kleiner*** sind als Z, die Eigenschaft haben, dafs, je nachdem sie mit s aufgehen oder nicht aufgehen, das Gleiche auch mit Z geschieht.

Auflösung. *A.* In (§. 32.) zeigte sich, dafs

$$1.\quad Z = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \ldots\ldots + x_2 A^2 + x_1 A + x_0$$

mit s ***aufgeht,*** oder nicht ***aufgeht,*** je nachdem die Zahl

$$2.\quad z = x_m r^m + x_{m-1} n r^{m-1} + x_{m-2} n^2 r^{m-2} + x_{m-2} n^3 r^{m-3} \ldots\ldots$$

$$\ldots\ldots + x_2 n^{m-2} r^2 + x_1 n^{m-1} r + x_0 n^m,$$

in deren Ausdruck

$$3.\quad nA = \mathfrak{S}s + r$$

n eine ***willkürliche*** zu s ***theilerfremde*** Zahl ist, mit s ***aufgeht*** oder ***nicht aufgeht.***

B. Dieser Satz kann zur Auflösung der gegenwärtigen Aufgabe dienen. Denn da r in (3.), wenn man es den ***echten*** positiven oder negativen Rest zu s sein läfst, jedenfalls $< s$, und wenn man für r den ***unbedingt echten*** Rest zu s nimmt, sogar $< \frac{1}{2}s$ ist, und man von den Multiplicatoren der x in (2.) wiederum nur die echten Reste zu s zu nehmen braucht: so sind die Multiplicatoren der x in (2.) immer kleiner als in (1.), und folglich ist immer z kleiner als Z. Der Ausdruck (1.) für Z aber drückt nach (§. 30.) jede beliebige Zahl aus, und es ist nicht nöthig, dafs man grade, wie im dekadischen System, $A = 10$ setzt, sondern es kann für A willkürlich eben sowohl $10^2 = 100$, $10^3 = 1000$ und so weiter genommen werden. Setzt man $A = 10$, so sind die x blofs einfache Ziffern < 10. Setzt man $A = 100$, so sind die x Zahlen von 2 Ziffern und < 100. Überhaupt sind die x, wenn man $A = 10^k$ setzt, Zahlen von k Ziffern, aber jedenfalls $< A$. Für das dekadische Zahlensystem heifst die Gleichung (3.) allgemein

$$4.\quad n.10^k = \mathfrak{S}s + r,$$

und in dieser Gleichung sind die ***beiden*** Zahlen k und n ***willkürlich.***

C. Da nun z (2.) ***um so kleiner*** sein wird, je kleiner r und n sind, insofern nicht k wiederum die x sehr grofs macht, so wird man die willkürlichen n und k so anzunehmen suchen müssen, dafs die r und n möglichst klein sind. Am ***vortheilhaftesten*** ist es offenbar, wenn r und n beide $= 1$ sein können; und ***gut,*** wenn wenigstens eins von ihnen $= 1$ ist.

D. Wenn s eine ***theilbare*** Zahl ist, so darf man eigentlich nur untersuchen, ob diejenigen ***Stammzahlen,*** oder diejenigen Potenzen von ***Stammzahlen,*** welche die Factoren von s sind, in Z aufgehen oder nicht. Denn wenn alle diese Factoren in Z aufgehen, so geht auch s in Z auf (§. 26.). Doch hindert nichts, auch s ***auf einmal*** in Rechnung zu bringen, wenn man

nur für n Zahlen setzt, die mit s keinen Theiler gemein haben. Vor Allem kommt es indessen auf die *Stammzahlen* an.

E. Auch kann, wenn ja z noch eine sehr *grofse* Zahl ist, auf dieselbe das Verfahren *wiederholt angewendet werden*, um zu noch *kleineren* Zahlen zu gelangen, mit welchen *zugleich* Z mit s aufgehe oder nicht aufgehe.

Beispiele.

No. 1. Es sei

$$s = 3 \quad \text{und} \quad s = 3^2 = 9.$$

Für diese beiden Werthe von s ist schon

$$5. \quad 10 = \mathfrak{G}.3+1 = \mathfrak{G}.9+1;$$

also $n=1$, $k=1$, $r=1$ und in (2.)

$$6. \quad z = x_0+x_1+x_2\ldots\ldots+x_m,$$

wo, wegen $k=1$, die x die *blofsen Ziffern* von Z sind. Also geht die Zahl Z mit 3 und 9 auf, wenn die *Summe ihrer Ziffern* mit 3 und 9 aufgeht; wie bekannt.

No. 2. Es sei

$$s = 27 = 3^3.$$

Hier ist

$$7. \quad 10^3 = 37.27+1 = \mathfrak{G}.27+1;$$

also ist hier $n=1$, $k=3$ und $r=1$, und folglich in (2.) wieder

$$8. \quad z = x_0+x_1+x_2\ldots\ldots+x_m,$$

wo aber, wegen $k=3$, die x die Zahlen sind, welche je *drei Ziffern* von Z von der Rechten zur Linken ausdrücken. Folglich geht Z mit 27 auf, wenn die *Summe jener Zahlen* x mit 27 aufgeht.

Wäre z. B.

$$9. \quad Z = 25084365147,$$

so wäre

$$10. \quad z = 147+365+84+25 = 621.$$

Dieses z geht mit 27 auf, also mufs auch Z mit 27 aufgehen; was auch der Fall ist.

No. 3. Es sei

$$s = 81 = 3^4.$$

Hier ist

$$11. \quad 10^9 = 12345679.81+1 = \mathfrak{G}.81+1,$$

also ist hier $n=1$, $k=9$, $r=1$ und in (2.) wieder

$$12. \quad z = x_0+x_1+x_2\ldots\ldots+x_m,$$

wo, wegen $k=9$, die x die Zahlen sind, welche je *neun* Ziffern von Z

von der Rechten zur Linken ausdrücken, und $\mathbf{Z}$ geht mit 81 auf, wenn die *Summe* dieser Zahlen mit 81 aufgeht.

Da aber z hier schon wenigstens 9 Ziffern hat, und also sehr grofs ist, so mag man (4.) anders anzuwenden versuchen.

Es ist

$$13.\quad 8.10 = \mathfrak{G}.81-1,$$

also $n=8$, $k=1$, $r=-1$. Dieses giebt zunächst in (2.)

$$14.\quad z = (-1)^m[x_m - n x_{m-1} + n^2 x_{m-2} - n^3 x_{m-3} \dots \pm n^{m-1} x_1 \mp n^m x_0].$$

Sodann ist (nach §. 11. Anm. gerechnet, nemlich die echten Reste ϱ der Multiplicatoren der x genommen):

$$15.\quad \begin{cases} n = 8, & \text{also } \varrho_m = +8, \\ n^2 = \mathfrak{G}.81-17, & \text{also } \varrho_{m-1} = -17, \\ n^3 = \mathfrak{G}.81+26, & \text{also } \varrho_{m-2} = +26, \\ n^4 = \mathfrak{G}.81-35, & \text{also } \varrho_{m-3} = -35, \\ n^5 = \mathfrak{G}.81-37, & \text{also } \varrho_{m-4} = -37, \\ n^6 = \mathfrak{G}.81+28, & \text{also } \varrho_{m-5} = +28, \\ n^7 = \mathfrak{G}.81-19, & \text{also } \varrho_{m-6} = -19, \\ n^8 = \mathfrak{G}.81+10, & \text{also } \varrho_{m-7} = +10, \\ n^9 = \mathfrak{G}.81-1, & \text{also } \varrho_{m-8} = -1; \end{cases}$$

(Die folgenden ϱ sind wieder dieselben; nur haben sie entgegengesetzte Zeichen.)

folglich ist in (14.)

$$16.\quad z = \pm[x_m - 8.x_{m-1} - 17.x_{m-2} - 26.x_{m-3} - 35.x_{m-4} + 37.x_{m-5} + 28.x_{m-6} + 19.x_{m-7} + 10.x_{m-8} + \dots],$$

wo die x die blofsen Ziffern der Zahl $\mathbf{Z}$ von der Linken zur Rechten sind.

Wäre z. B.

$$17.\quad \mathbf{Z} = 7943949936972,$$

so wäre nach (16.)

$$z = \pm[7-8.9-17.4-26.3-35.9+37.4+28.9+19.9+10.3 +1.6-8.9-17.7-26.2] \text{ oder}$$

$$21.\quad z = \pm[7-72-68-78-315+148+252+171+30+6-72-119-52] = \pm(614-776) = \mp 162.$$

Dieses z geht mit 81 auf, also mufs auch $\mathbf{Z}$ (17.) mit 81 aufgehen; was auch der Fall ist.

No. 4. Es sei

$$s = 7.$$

Hier ist

$$19.\quad 10^3 = 143.7-1,$$

also $n = 1$, $k = 3$ und $r = 1$ und in (2.)

$$20. \quad z = x_0 - x_1 + x_2 - x_3 \ldots \pm x_m,$$

wo die x die 3ziffrigen Zahlen in Z von der Rechten zur Linken sind.

Wäre z. B.

$$21. \quad Z = 80939417280533,$$

so wäre zufolge (20.)

$$22. \quad z = 533 - 280 + 417 - 939 + 80 = 1030 - 1219 = -189.$$

Dieses z geht mit 7 auf; also auch Z.

Wollte man (4.) anwenden, so könnte man setzen

$$23. \quad 5.10 = \mathfrak{G}.7 + 1;$$

also wäre $n = 5$, $k = 1$ und $r = 1$. Dieses giebt für z in (2.)

$$24. \quad z = x_m + n x_{m-1} + n^2 x_{m-2} + n^3 x_{m-3} \ldots + n^m x_0.$$

Nun ist

$$25. \quad \begin{cases} n = \mathfrak{G}.7 - 2, & n^4 = \mathfrak{G}.7 + 2, & n^7 = \mathfrak{G}.7 - 2, \\ n^2 = \mathfrak{G}.7 - 3, & n^5 = \mathfrak{G}.7 + 3, & n^8 = \mathfrak{G}.7 - 3, \quad \text{u. s. w.} \\ n^3 = \mathfrak{G}.7 - 1, & n^6 = \mathfrak{G}.7 + 1, & n^9 = \mathfrak{G}.7 - 1, \end{cases}$$

also in (24.)

$$z = x_m - 2x_{m-1} - 3x_{m-2} - x_{m-3} + 2x_{m-4} + 3x_{m-5} + x_{m-6} \ldots \text{ oder}$$

$$26. \quad z = x_m - x_{m-3} + x_{m-6} - x_{m-9} \ldots - 2(x_{m-1} - x_{m-4} + x_{m-7} \ldots) - 3(x_{m-2} - x_{m-5} + x_{m-8} \ldots),$$

wo die x die einfachen Ziffern von Z sind. Dieser Ausdruck giebt z. B. für die Zahl Z (21.)

$$z = 8 - 3 + 1 - 8 + 3 - 2(0 - 9 + 7 - 0 + 3) - 3(9 - 4 + 2 - 5) \text{ oder}$$

$$27. \quad z = +1 - 2(+1) - 3(+2) = +1 - 2 - 6 = -7.$$

Dieses z geht mit 7 auf; also auch Z.

No. 5. Es sei

$$s = 11.$$

Hier ist

$$28. \quad 10 = \mathfrak{G}.11 - 1 \quad \text{und} \quad 10^2 = \mathfrak{G}.11 + 1,$$

also $n = 1$ und $r = -1$ für $k = 1$, $r = +1$ für $k = 2$. Mithin giebt (2.)

$$29. \quad z = -x_m + x_{m-1} - x_{m-2} + x_{m-3} \ldots,$$

wo die x die einfachen Ziffern von Z sind, und

$$30. \quad z = x_m + x_{m-1} + x_{m-2} + x_{m-3} \ldots,$$

wo die x die *zweiziffrigen* Zahlen in Z von der Rechten zur Linken bedeuten.

Z. B. für

$$31. \quad Z = 37201458690434819$$

giebt (29.)

$$32.\quad z = -3+7-2+0-1+4-5+8-6+9-0+4-3+4-8+1-9 = -37+37 = 0$$

und (30.) giebt

$$33.\quad z = 19+48+43+90+86+45+1+72+3 = 407$$

und, *wiederholt* angewendet,

$$34.\quad z = 4+07 = 11.$$

Diese z gehen mit 11 auf; also geht auch $\mathbf{Z}$ (31.) mit 11 auf.

No. 6. Es sei

$$s = 13.$$

Hier ist

$$35.\quad 10^3 = 77.13-1 = \mathfrak{G}.13-1,$$

also $n=1$, $k=3$, $r=-1$, mithin nach (2.)

$$36.\quad z = x_0 - x_1 + x_2 - x_3 \ldots \pm x_m,$$

wo die x die *dreiziffrigen* Zahlen in $\mathbf{Z}$ von der Rechten zur Linken sind; eben wie in No. 4. für $s=7$.

Will man (4.) anwenden, so kann man setzen:

$$37.\quad 4.10 = \mathfrak{G}13+1,$$

also $n=4$, $k=1$, $r=+1$, folglich in (2.)

$$38.\quad z = x_m + 4x_{m-1} + 4^2.x_{m-2} + 4^3.x_{m-3} \ldots,$$

und da

$$39.\quad \begin{cases} n = \mathfrak{G}s+4, & n^4 = \mathfrak{G}s-4, \quad n^7 = \mathfrak{G}s+4, \\ n^2 = \mathfrak{G}s+3, & n^5 = \mathfrak{G}s-3, \quad n^8 = \mathfrak{G}s+3, \quad \text{u. s. w.} \\ n^3 = \mathfrak{G}s-1, & n^6 = \mathfrak{G}s+1, \quad n^9 = \mathfrak{G}s-1, \end{cases}$$

ist,

$$z = x_m + 4x_{m-1} + 3x_{m-2} - x_{m-3} - 4x_{m-4} - 3x_{m-5} \ldots \text{ oder}$$

$$40.\quad z = (x_m - x_{m-3} + x_{m-6} - x_{m-9} \ldots) + 4(x_{m-1} - x_{m-4} + x_{m-7} \ldots) + 3(x_{m-2} - x_{m-5} + x_{m-8} \ldots),$$

wo die x die einfachen Ziffern von $\mathbf{Z}$ sind.

Wäre z. B.

$$41.\quad \mathbf{Z} = 5891476201146758014,$$

so würde (36.)

$$42.\quad z = 14-758+146-201+476-891+5 = 641-1850 = -1209$$

und, *wiederholt* angewendet,

$$43.\quad z = 209-1 = 208$$

geben. Hingegen (40.) würde geben:

$$z = 5-1+6-1+6-8+4+4(8-4+2-1+7-0)$$
$$+3(9-7+0-4+5-1) \text{ oder}$$

44. $z = 21-10+4(17-5)+3(14-12) = 11+48+6 = 65.$

Die z (43. und 44.) gehen mit $s=13$ auf; also auch $\mathbf{Z}$ (41.).

No. 7. Es sei

$$s = 17.$$

Hier kann man setzen:

45. $10^2 = \mathfrak{G}.17-2,$

also

46. $n = 1, \quad k = 2, \quad r = -2.$

Dieses giebt in (2.)

$$z = x_0 - 2x_1 + 2^2.x_2 - 2^3 x_3 + 2^4 x_4 \ldots. \text{ oder}$$
$$z = x_0 - 2x_1 + 4x_2 - 8x_3 - x_4 + 2x_5 - 4x_6 + 8x_7 + x_8 \ldots. \text{ oder}$$

47. $z = (x_0 - x_4 + x_8 - x_{12} \ldots.) - 2(x_1 - x_5 + x_9 \ldots.) + 4(x_2 - x_6 + x_{10} \ldots.)$
$$- 8(x_3 - x_7 + x_{11} \ldots.),$$

wo die x die *zweiziffrigen* Zahlen in $\mathbf{Z}$ von der Rechten zur Linken sind.

Setzt man dagegen in (4.) $n=5$, $k=1$, so erhält man

48. $5.10 = \mathfrak{G}.17-1$ also $r = -1.$

Dieses giebt in (2.)

$$z = -x_m + 5x_{m-1} - 5^2 x_{m-2} + 5^3 x_{m-3} - 5^4 x_{m-4} \ldots. \text{ oder}$$

49. $z = -x_m + 5x_{m-1} - 8x_{m-2} + 6x_{m-3} + 4x_{m-4} - 3x_{m-4} + 2x_{m-5}$
$$-7x_{m-6} - x_{m-7} + 5x_{m-8} \ldots.,$$

wo x die einfachen Ziffern von $\mathbf{Z}$ sind.

Es sei z. B.

50. $\mathbf{Z} = 308791540229761043805,$

so giebt (47.)

$$z = 5-2.38+4.4-8.61-97+2.22-4.40+8.15+79-2.8+4.3$$

oder

$$z = 5+16+44+120+79+12-(76+488+97+160+16) \text{ oder}$$
$$z = 276-837 = -561$$

und, wiederholt angewendet,

51. $z = 61-25 = 51.$

Hingegen (49.) giebt

$$z = -3+0-64+42+36-3+10-28-0+10-16+54+28-18$$
$$+2-0-4+15-64+0+20 \text{ oder}$$

52. $z = 217-200 = 17.$

Beide $\mathbf{Z}$ (51. u. 52.) gehen mit $s=17$ auf; also geht auch $\mathbf{Z}$ (50.) mit 17 auf

No. 8. Es sei

$$s = 19.$$

Hier kann man in (4.) $n = 2$, $k = 1$ setzen. Dieses giebt

53. $$2.10 = \mathfrak{G}19 + 1, \text{ also } r = 1,$$

folglich in (2.)

$$z = x_m + 2x_{m-1} + 2^2 x_{m-2} + 2^3 x_{m-3} + 2^2 x_{m-4} \dots \text{ oder}$$

54. $$z = x_m + 2x_{m-1} + 4x_{m-2} + 8x_{m-3} - 3x_{m-4} - 6x_{m-5} + 7x_{m-6} - 5x_{m-6} + 9x_{m-7} - x_{m-7} - 2x_{m-1} - 4x_{m-2} \dots.$$

Es sei z. B.

55. $$Z = 13413966072992,$$

so giebt (54.)

$$z = 1 + 6 + 16 + 8 - 9 - 54 + 42 - 30 + 0 - 7 - 4 - 36 - 72 + 6 \text{ oder}$$

$$z = 79 - 212 = -133$$

und, wiederholt angewendet,

56. $$z = 1 + 6 + 12 = 19.$$

Dieses z geht mit 19 auf; also auch Z.

F. Es würde nützlich sein, nach dieser Art eine *Tafel,* wenigstens für alle Stammzahlen, etwa bis 1000, zu berechnen.

Für eine solche Tafel würde es immer am besten sein, in (4.) n *stets* $= 1$ zu setzen. Ein anderer Werth von n kann zwar, wie sich an den obigen Beispielen zeigt, in einzelnen Fällen nützlich sein, aber wenn man eine voraus berechnete *Tafel* der Multiplicatoren der x in (2.) hat, nemlich eine Tafel der *echten Reste* der Multiplicatoren r^m, nr^{m-1}, n^2r^{m-2} etc. zu s, so ist es gleichgültig, was r in (4.) für $n = 1$ ist: immer sind die Reste $< \frac{1}{2}s$. Aufserdem aber hat man, wenn immer $n = 1$ ist, noch den Vortheil, dafs, wenn Z *nicht* mit s aufgeht, z auch *denselben Rest* läfst wie Z, so dafs man also in solchem Falle *auch noch sogleich den Rest der Division von Z mit s findet;* was nicht unmittelbar geschieht, wenn n *nicht* gleich 1 ist. Für $n = 1$ nemlich giebt (9. §. 32.) blofs

57. $$Z = \mathfrak{G}s + z,$$

und es folgt daraus, dafs, wenn man $Z = \mathfrak{G}s + \varrho_1$ und $z = \mathfrak{G}s + \varrho_2$ setzt, wo ϱ_1 und ϱ_2 beides die *unbedingt echten* Reste bezeichnen,

58. $$\mathfrak{G}s + \varrho_1 = \mathfrak{G}s + \mathfrak{G}s + \varrho_2 = \mathfrak{G}s + \varrho_2$$

sein mufs; was nicht anders sein kann, als wenn ϱ_1 *gleich* ϱ_2 ist, indem es *nur einen* unbedingt echten Rest zu s giebt.

Ferner wird es für die *Tafel* auch gut sein, in (4.) *k stets gleich* 1 zu setzen: denn in (2.), welches sich für $n = 1$ auf

59. $$z = x_m r^m + x_{m-1} r^{m-1} + x_{m-2} r^{m-2} + x_{m-3} r^{m-3} \ldots + x_1 r + x_0,$$

oder, wenn man die unbedingt echten Reste r^m, r^{m-1}, r^{m-2}, ... durch ϱ_m, ϱ_{m-1}, ϱ_{m-2}, ... bezeichnet, auf

60. $$z = x_m \varrho_m + x_{m-1} \varrho_{m-1} + x_{m-2} \varrho_{m-2} \ldots + x_1 \varrho_1 + x_0$$

reducirt, sind die Multiplicatoren ϱ der x *immer* $< \frac{1}{2} s$. Ist nun $k = 1$, so sind die x in (1.) oder (60.) die *einzelnen Ziffern* der Zahl Z, und z (60.) hat so viele Glieder als die Zahl Z einzelne Ziffern. Es kann also von dem ϱ *nur das 1* bis *9fache* zu nehmen vorkommen. Ist dagegen $k > 1$, so hat zwar z in (60.) *weniger Glieder*, aber die x sind nun *mehrziffrige* Zahlen; eben wie die ϱ; letzteres wenn s einigermafsen grofs ist. Mehrziffrige Zahlen mit *einander* zu multipliciren, wird aber, selbst wenn es *weniger oft* vorkommt, doch immer schwieriger sein, als blofs die 1 bis 9fachen der mehrziffrigen Zahlen ϱ zu nehmen. Für *eine Tafel* ist das letztere aber noch *um so mehr* passend, da sich auch recht gut die 1 bis 9fachen der ϱ vorausberechnen lassen und sogleich in die Tafel aufgenommen werden können, nicht aber wohl die 1 bis 100 oder die 1 bis 1000fachen u. s. w. Enthält nun die Tafel auf diese Weise sogleich die 1 bis 9fachen der ϱ, im Voraus berechnet, so ist für z (60.) *gar keine Multiplication* weiter nöthig, sondern man kann die einzelnen Glieder der Reihe rechts in (60.) aus der Tafel unmittelbar *ablesen* und braucht nur die positiven wie die negativen Glieder zusammen- und die beiden Summen von einander abzuziehen.

G. Für die Tafel also würde man $n = 1$ und $k = 1$, folglich in (4.) blofs

61. $$10 = \mathfrak{G} s + r$$

zu setzen haben, welches, wenn $s > 10$ ist, gradezu $r = 10$ giebt. Also sind dann die ϱ in (60.) nichts andres als die *unbedingt echten* Reste der verschiedenen Potenzen von 10 selbst, zu s.

Für die Urzahl $s = 857$ z. B. wäre

62. $$\begin{cases} 10 = \mathfrak{G}.857 + \varrho_1 & \text{und} \quad \varrho_1 = +\ 10, \\ 10^2 = \mathfrak{G}.857 + \varrho_2 & \text{-} \quad \varrho_2 = +\ 100, \\ 10^3 = \mathfrak{G}.857 + \varrho_3 & \text{-} \quad \varrho_3 = +\ 143, \\ 10^4 = \mathfrak{G}.857 + \varrho_4 & \text{-} \quad \varrho_4 = -\ 284, \\ 10^5 = \mathfrak{G}.857 + \varrho_5 & \text{-} \quad \varrho_5 = -\ 269, \\ \ldots\ldots & \text{-} \quad \ldots\ldots \end{cases}$$

Es würde daher, um zu finden, ob eine gegebene Zahl Z mit 857 aufgehe oder nicht, und welcher ***Rest*** im letzten Fall bleibe, von den Ziffern der Zahl Z, von der Rechten nach der Linken zu, die ***erste*** mit $+10$, die ***zweite*** mit $+100$, die ***dritte*** mit $+143$, die ***vierte*** mit -284, die ***fünfte*** mit -269 u. s. w. zu multipliciren sein, und die algebraische Summe dieser Producte würde z (60.) geben. Je nachdem dieses z mit 857 aufgeht, oder nicht, geht auch die gegebene Zahl Z mit 857 auf, oder nicht; und wenn z ***nicht*** mit 857 aufgeht, so ist der ***unbedingt echte*** Rest von z zu 857 ***derselbe,*** wie der von Z.

Aber auch die 1 bis 9fachen der ϱ (62.), die vorkommen können, braucht man nicht so wie sie sind zu nehmen, sondern auch von ihnen nur die ***unbedingt echten Reste*** zu $s=857$. So würde man z. B. für die Vielfachen von $\varrho_4=-284$ nicht -284, -568, -852, -1136 u. s. w., sondern vielmehr nur -284, $+289$, $+5$, -279 u. s. w. zu nehmen haben. Findet man nun diese Vielfachen in der Tafel, so ist für z (60.) ***gar keine Multiplication*** weiter nöthig, sondern nur die ***Addition*** von Zahlen, die sich, ganz ausgerechnet, in der Tafel finden.

Die Tafel würde für die Stammzahl $s=857$ Folgendes geben.

63.

Nummer der Ziffern von der Rechten zur Linken.	Werth der Ziffern. 1	2	3	4	5	6	7	8	9
1 ...	+ 1	+ 2	+ 3	+ 4	+ 5	+ 6	+ 7	+ 8	+ 9
2 ...	+ 10	+ 20	+ 30	+ 40	+ 50	+ 60	+ 70	+ 80	+ 90
3 ...	+100	+200	+300	+400	−357	−257	−157	− 57	+ 43
4 ...	+143	+286	−428	−285	−142	+ 1	+144	+287	−427
5 ...	−284	+289	+ 5	−279	+294	+ 10	−274	+299	+ 15
6 ...	−269	+319	+ 50	−219	+369	+100	−169	+419	+150
7 ...	−119	−238	−357	+381	+262	+143	+ 24	− 95	−214
8 ...	−333	+191	−142	+382	+ 49	−284	+240	− 93	−426
9 ...	+ 98	+196	+294	+392	−367	−269	−171	− 73	+ 25
10 ...	+123	+246	+369	−365	−242	−119	+ 4	+127	+250
11 ...	+373	−111	+262	−222	+151	−333	+ 40	+413	− 71
12 ...	+302	−253	+ 49	+351	−204	+ 98	+400	−155	+147
13 ...	−408	+ 41	−367	+ 82	−326	+123	−285	+164	−244
14 ...	+205	+410	−242	− 37	+168	+373	−279	− 74	+131
15 ...	+336	−185	+151	−370	− 34	+302	−219	+117	−404
16 ...	− 68	−136	−204	−272	−340	−408	+381	+313	+245
17 ...	+177	+354	−326	−119	+ 28	+205	+382	−298	−121
18 ...	+ 56	+112	+168	+224	+280	+336	+392	−409	−353
19 ...	−297	+263	− 34	−331	+229	− 68	−365	+195	−102
20 ...	−399	+ 59	−340	+118	−281	+177	−222	+236	−163
21 ...	+295	−267	+ 28	+323	−239	+ 56	+351	−211	+ 84
22 ...	+379	− 99	+280	−198	+181	−297	+ 82	−396	− 17
23 ...	+362	−133	+229	−266	+ 96	−399	− 37	+325	−170
24 ...	+192	+384	−281	− 89	+103	+295	−370	−178	+ 14

Wenn nun z. B.

$$64. \quad Z = 804739885214799049628954$$

wäre, so hätte man wie folgt zu rechnen:

65.

Für die	Ziffer			Für die	Ziffer		
1te	Ziffer	4 ...	$+4$	7te	Ziffer	9 ...	-214
- - 2te	-	5 ...	$+50$	- - 11te	-	9 ...	-71
- - 3te	-	9 ...	$+43$	- - 15te	-	2 ...	-185
- - 4te	-	8 ...	$+287$	- - 16te	-	5 ...	-340
- - 5te	-	2 ...	$+289$	- - 17te	-	8 ...	-298
- - 6te	-	6 ...	$+100$	- - 18te	-	8 ...	-409
- - 8te	-	4 ...	$+382$	- - 19te	-	9 ...	-102
- - 10te	-	9 ...	$+250$	- - 20te	-	3 ...	-340
- - 12te	-	7 ...	$+400$	- - 22te	-	4 ...	-198
- - 13te	-	4 ...	$+82$	- - 24te	-	8 ...	-178
- - 14te	-	1 ...	$+205$			Thut zusammen	-2335
- - 21te	-	7 ...	$+351$				$+2443$
		Thut zusammen	$+2443$			Bleibt	$+108$

Die Zahl **Z** (64.) kann also mit $s = 857$ *nicht* aufgehen, sondern es mufs der Rest $+108$ bleiben; und so verhält es sich auch.

§. 34.

Lehrsatz.

Es seien u *und* v *zwei beliebige, zu einander theilerfremde positive ganze Zahlen.*

I. *Setzt man in der Gleichung*

$$1. \quad mv = nu + r$$

der Reihe nach

$$2. \quad m = 0, 1, 2, 3, 4, \ldots . u - 1$$

und nimmt für alle r *die positiven oder die negativen echten Reste, deren zeichenfreie Werthe also alle* $< u$ *sind, so ist kein* r *dem andern gleich, und die zeichenfreien Werthe von* r *sind nothwendig alle die Zahlen*

$$3. \quad r = 0, 1, 2, 3, 4, \ldots . u - 1,$$

obwohl in anderer Aufeinanderfolge als die von m.

Zugleich sind alle $n < v$, *wenn* $v > u$ *ist. Ist* $v < u$, *so ist für diejenigen negativen* r, *welche mit* v *aufgehen und die sich dann unter den Werthen* (3.) *von* r *befinden,* $n = v$.

Zu dem Werth 0 *von* m *gehört* $r = 0$, *und zu* $r = 0$ *gehört* $m = 0$ *und* $n = 0$.

II. *Für jedes beliebige positive oder negative* r *in* (1.), *auch* $r = 0$ *nicht ausgenommen, so dafs also* r *allgemein durch*

$$4.\quad r = \varepsilon u + r_0$$

ausgedrückt werden kann, wo ε *eine ganze positive oder negative Zahl und* r_0 *eine der Zahlen* (3.) *ist, giebt es immer unzählige zusammengehörige ganzzahlige Werthe von* m *und* n, *welche der Gleichung* (1.) *genugthun. Sie werden allgemein durch*

$$5.\quad m = \lambda u + m_0 \quad \text{und}$$

$$6.\quad n = \lambda v + n_0 - \varepsilon$$

ausgedrückt, wo λ *willkürlich ist, das zu* r_0 *in* (1.) *gehörige* m_0 *aber immer eine der Zahlen*

$$7.\quad m_0 = 0, 1, 2, 3, \ldots u-1$$

und das zu r_0 *gehörige* n_0 *eine der Zahlen*

$$8.\quad n_0 = 0, 1, 2, 3, \ldots v-1$$

bezeichnet, mit Ausnahme von $r_0 = -v$ *für* $v < u$, *wo* $n_0 = v$ *ist. Aufser den durch* (5. u. 6.) *ausgedrückten Werthen von* m *und* n *giebt es aber keine andern.*

III. *Unter den unzähligen Werthen von* m *und* n (5. u. 6.), *die mit* r (4.) *der Gleichung* (1.) *genugthun, giebt es für jedes* r *immer einen und nur den einen positiven Werth* $m_0 < u$ *von* m *und ein und nur das eine negative* $m_0 - u$, *dessen zeichenfreier Werth* $u - m_0$ *ebenfalls* $< u$ *ist, aber nicht zugleich immer ein zugehöriges positives oder negatives* n, *dessen zeichenfreier Werth seinerseits* $< v$ *wäre, sondern letzteres nur in dem Falle, wenn in dem Ausdruck* (4.) *von* r, $\varepsilon = 0$, *also der zeichenfreie Werth von* r *eine der Zahlen* (3.) *ist. In diesem einen Falle sind auch die zeichenfreien Werthe der zu* m_0 *und* $m_0 - u$ *gehörigen Werthe* n_0 *und* $n_0 - v$ *von* n *aus den Zahlen* (8.), *und wenn* $v < u$ *ist, so ist für* $r =$ *den Vielfachen von* $-v$, *die* $< u$ *sind,* $n_0 = v$. *Wir wollen die Werthe* m_0 *und* $m_0 - u$ *von* m, *nebst dem zugehörigen* $n_0 - \varepsilon$ *und* $n_0 - \varepsilon - v$ *von* n *kleinste Wurzeln der Gleichung* (1.) *nennen.*

IV. *Wenn man dasjenige positive* $m < u$ *und das zugehörige positive* $n < v$, *welche in* (1.) *zu dem Rest* $r = +1$ *gehören, und welche nach* (III.) *immer Statt finden, durch* m_1 *und* n_1 *bezeichnet, so dafs also* m_1 *und* n_1 *zu dem Reste* $+1$ *die kleinsten positiven Wurzeln der Gleichung*

$$9.\quad mv = nu + 1$$

sind, so werden die kleinsten positiven und negativen Wurzeln der Gleichung* (1.) *zu einem beliebigen Rest* r *durch

$$10. \qquad m_0 = m_1 r - \tau u \quad \textit{und} \quad m_1 r - (\tau + 1) u \quad \textit{und}$$

$$11. \qquad n_0 - \varepsilon = n_1 r - \tau v \quad \textit{und} \quad n_1 r - (\tau + 1) v$$

ausgedrückt, wo τu ***in*** (10.) ***dasjenige Vielfache von*** u ***bedeutet, welches, von*** $m_0 r$ ***abgezogen, einen positiven Rest*** $m_1 < u$ ***läfst. In*** (11.) ***mufs*** τ ***denselben Werth bekommen, wie in*** (10.), ***wenn auch*** $n_0 r - \tau v$ ***nicht eine positive Zahl*** $< v$ ***ist.***

Beispiel. Es sei

$$12. \qquad v = 15, \quad u = 22.$$

Setzt man hier der Reihe nach $m = 0, 1, 2, 3, \ldots 21$, so ergiebt sich

$$13. \left\{\begin{array}{ll}
0.15 = 0.22 + 0 = 0.22 - 0 & 11.15 = 7.22 + 11 = 8.22 - 11 \\
1.15 = 0.22 + 15 = 1.22 - 7 & 12.15 = 8.22 + 4 = 9.22 - 18 \\
2.15 = 1.22 + 8 = 2.22 - 14 & 13.15 = 8.22 + 19 = 9.22 - 3 \\
3.15 = 2.22 + 1 = 3.22 - 21 & 14.15 = 9.22 + 12 = 10.22 - 10 \\
4.15 = 2.22 + 16 = 3.22 - 6 & 15.15 = 10.22 + 5 = 11.22 - 17 \\
5.15 = 3.22 + 9 = 4.22 - 13 & 16.15 = 10.22 + 20 = 11.22 - 2 \\
6.15 = 4.22 + 2 = 5.22 - 20 & 17.15 = 11.22 + 13 = 12.22 - 9 \\
7.15 = 4.22 + 17 = 5.22 - 5 & 18.15 = 12.22 + 6 = 13.22 - 16 \\
8.15 = 5.22 + 10 = 6.22 - 12 & 19.15 = 12.22 + 21 = 13.22 - 1 \\
9.15 = 6.22 + 3 = 7.22 - 19 & 20.15 = 13.22 + 14 = 14.22 - 8 \\
10.15 = 6.22 + 18 = 7.22 - 4 & 21.15 = 14.22 + 7 = 15.22 - 15
\end{array}\right.$$

Wäre dagegen

$$14. \qquad v = 22, \quad u = 15,$$

so wäre

$$15. \left\{\begin{array}{ll}
0.22 = 0.15 + 0 = 0.15 - 0 & 8.22 = 11.15 + 11 = 12.15 - 4 \\
1.22 = 1.15 + 7 = 2.15 - 8 & 9.22 = 13.15 + 3 = 14.15 - 12 \\
2.22 = 2.15 + 14 = 3.15 - 1 & 10.22 = 14.15 + 10 = 15.15 - 5 \\
3.22 = 4.15 + 6 = 5.15 - 9 & 11.22 = 16.15 + 2 = 17.15 - 13 \\
4.22 = 5.15 + 13 = 6.15 - 2 & 12.22 = 17.15 + 9 = 18.15 - 6 \\
5.22 = 7.15 + 5 = 8.15 - 10 & 13.22 = 19.15 + 1 = 20.15 - 14 \\
6.22 = 8.15 + 12 = 9.15 - 3 & 14.22 = 20.15 + 8 = 21.15 - 7 \\
7.22 = 10.15 + 4 = 11.15 - 11 &
\end{array}\right.$$

a. Wie (13. u. 15.) zeigen, sind die positiven, so wie die negativen Reste alle unter einander ***verschieden,*** und beide sind in (13.) die Zahlen 0, 1, 2, 3, ... 21 ($= u - 1$) und in (15.) die Zahlen 0, 1, 2, 3, ... 14

$(=u-1)$. Desgleichen sind in (15.), wo $v>u$ ist, alle n ohne Ausnahme $<v(=22)$. In (13.) dagegen, wo $v<u$, ist *für den* Rest $r=-u=-15$, $n=15=v$. Die übrigen n sind ebenfalls alle $<v$. Desgleichen gehört überall zu $m=0$, $r=0$, und zu $r=0$ gehört $m=0$ und $n=0$. Dieses zusammen ist was (I.) behauptet.

b. Es sei für (12.)

16. $r=141=6.u+9$, also in (4.) $\varepsilon=6$, $r_0=9$.

Die zu $r_0=9$ gehörigen m_0 und n_0 sind zufolge (13.) $=5$ und 3: also ist nach (5. u. 6.)

17. $$\begin{cases} m=\pm(1,2,3,\ldots)22+5 \text{ und} \\ n=\pm(1,2,3,\ldots)15+3-6 = (1,2,3,\ldots)15-3. \end{cases}$$

Man setze z. B. das *willkürliche* λ in (4. u. 5.) $=4$, so ist nach (17.)

18. $$\begin{cases} m=4.22+5=93 \text{ und} \\ n=4.15-3=57. \end{cases}$$

Diese m und n müssen also der Gleichung (1.) zu $r=141$ genugthun, das heifst, es mufs

19. $$93.15=57.22+141$$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (17.) sind diejenigen für $\lambda=0$, also $m=5<u$ und $n=-3$, welches die Werthe $m_0=5$ und $n_0-\varepsilon=3-6=-3$ *selbst* sind; desgleichen sind es diejenigen für $\lambda=-1$, also $m=-17$ und $n=-18$, wo der zeichenfreie Werth 17 von m ebenfalls $<u$ ist. Also müssen auch die Werthe 5 und -17 von m, und -3 und -18 von n der Gleichung (1.) zu dem Rest $r=141$ genugthun, das heifst, es mufs

20. $$\begin{cases} +5.15=-3.22+141 \text{ und} \\ -17.15=-18.22+141 \end{cases}$$

sein; was auch der Fall ist.

c. Es sei für (14.)

21. $r=-55=-4.u+5$, so dafs in (4.) $\varepsilon=-4$, $r_0=5$.

Die zu $r_0=5$ gehörigen m_0 und n_0 sind zufolge (15.) $=5$ und 7, also ist nach (5. u. 6.)

22. $$\begin{cases} m=\pm(1,2,3,\ldots)15+5 \text{ und} \\ n=\pm(1,2,3,\ldots)22+7+4. \end{cases}$$

Man setze das *willkürliche* λ in (4. u. 5.) $=-2$, so ist nach (22.)

$$23.\quad \begin{cases} m = -2.15+5 = -25 \text{ und} \\ n = -2.22+11 = -33 \end{cases}$$

Diese m und n müssen der Gleichung (1.) zu $r=-55$ genugthun, das heifst, es mufs

$$24.\quad -25.22 = -33.15-55$$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (22.) sind wieder diejenigen für $\lambda=0$, also $m=5<u$ und $n=11$, welches die Werthe von $m_0=5$ und $n_0-\varepsilon=7-(-4)=11$ *selbst* sind; desgleichen sind es diejenigen für $\lambda=-1$, also $m=-10$ und $n=-11$, wo der zeichenfreie Werth 10 von m ebenfalls $<u$ ist. Also müssen auch die Werthe 5 und -10 von m und 11 und -11 von n der Gleichung (1.) zu dem Reste $r=-55$ genugthun, das heifst es mufs

$$25.\quad \begin{cases} +5.22 = +11.15-55 \text{ und} \\ -10.22 = -11.15-55 \end{cases}$$

sein; was auch der Fall ist.

Die Resultate in (*b.* u. *c.*) sind den Behauptungen in (II. u. III.) gemäfs.

d. Für (12.) ist zufolge (13.) dasjenige m und n, welches dem Rest $+1$ entspricht, $=3$ und 2, so dafs also für (12.)

$$26.\quad m_1 = 3 \text{ und } n_1 = 2$$

ist. Nun sei, wie in (16.),

$$27.\quad r = 141,$$

so giebt (10. u. 11.)

$$28.\quad \begin{cases} m_0=3.141-19.22=+5, \text{ also } \tau=19 \text{ und } m_0=3.141-20.22=-17 \text{ und} \\ n_0=2.141-19.15=-3 \text{ und } \qquad n_0=2.141-20.15=-18, \end{cases}$$

und diese m_0 und n_0 müssen der Gleichung (1.) für den Rest $r=141$ genugthun; was auch zufolge (20.) der Fall ist.

e. Für (14.) ist zufolge (15.) dasjenige m und n, welches dem Rest $+1$ entspricht $=13$ und 19, so dafs also für (14.)

$$29.\quad m_1 = 13 \text{ und } n_1 = 19$$

ist. Nun sei, wie in (21.),

$$30.\quad v = -55,$$

so giebt (10. und 11.)

$$31.\quad \begin{cases} m_0=-13.55+48.15=+5, \text{ also } \tau=-48 \text{ und } m_0=-13.55+47.15=-10 \text{ und} \\ n_0=-19.55+48.22=+11 \text{ und } \qquad n_0=-19.55+47.22=-11, \end{cases}$$

und diese m_0 und n_0 müssen der Gleichung (1.) für den Rest $r=-55$ genugthun; was auch zufolge (25.) der Fall ist.

Die Resultate (*d.* u. *e.*) sind den Behauptungen in (IV.) gemäfs.

Beweis. *A.* Gäben zwei verschiedene m, z. B. m_β und m_γ, beide $<u$, mit den dazu gehörigen n_β und n_γ *ein und dasselbe* r, so dafs also

$$32.\quad \begin{cases} m_\beta v = n_\beta u \pm r \text{ und} \\ m_\gamma v = n_\gamma u \pm r \end{cases}$$

wäre, so würde daraus

$$33.\quad (m_\beta - m_\gamma)v = (n_\beta - n_\gamma)u$$

folgen, und also müfste $m_\beta - m_\gamma$ mit u *aufgehen*, da v nach der Voraussetzung keinen Theiler mit u gemein hat (§. 25.) Dieses kann aber nicht sein, da m_β und m_γ beide $<u$ sind und folglich auch $m_\beta - m_\gamma < u$ ist. Also können keine zwei m, beide $<u$, *einen und denselben* Rest $\pm r$ lassen, und folglich sind *alle* zu $m = 1, 2, 3, \ldots u-1$ gehörigen r *von einander verschieden.*

Die *Anzahl* der r ist aber der der Werthe von m *gleich*, und folglich $= u$. Zugleich sollen die zeichenfreien Werthe aller $r < u$ sein. Also sind diese zeichenfreien Werthe der r nothwendig *alle* die u Zahlen 0, 1, 2, 3, ... $u-1$ selbst; gemäfs (3.)

B. Der *gröfste* Werth von n findet in (1.) offenbar für den *gröfsten* Werth von m Statt, also für $m = u-1$. Man setze für $m = u-1$ in (1.)

$$34.\quad (u-1)v = xu + r.$$

Soll hier r *positiv* sein, so kann x nicht $= v$ sein, selbst nicht für $r = 0$; denn $x = v$ würde immer $xu = vu > (u-1)v$ geben. Folglich ist für *positive* r, x, also n, *immer* $<v$.

Soll r *negativ* sein, so folgt aus

$$35.\quad (u-1)v = v.u - v = (v+\varkappa)u - (\varkappa u + v),$$

dafs nur dann

$$36.\quad n = v + \varkappa$$

sein kann, wenn

$$37.\quad \varkappa u + v < u$$

ist; denn der absolute Werth $\varkappa u + v$ des Restes in (35.) soll *immer* $<u$ sein. Die Bedingung (37.) ist aber nur für $\varkappa = 0$ erfüllbar; denn für *jedes* gröfsere $\varkappa$ ist $\varkappa u + v$ nicht $<u$, sondern $>u$, was auch v sein mag. *Nie* also kann zufolge (36.) $n > v$ sein. Es kann höchstens $= v$ sein, und dieses zufolge (37.) nur dann wenn $v < u$ ist. Nun ist für ein *beliebiges* $u - \mu$fache von v:

$$38.\quad (u-\mu)v = v.u - \mu v.$$

Ist nun $v < u$, so kann auch noch $\mu v < u$ sein. Also für alle die Reste $-v$, $-2v$, $-3v$, ... $-\mu v$, die auch *alle* vorkommen, ist $n = v$.

Zusammen also folgt, daſs n für $v > u$ *immer* $< v$ ist; desgleichen auch für $v < u$, ausgenommen wenn der *negative Rest* mit v aufgeht; wie solches der Lehrsatz in (1.) behauptet.

C. Ist $m = 0$, so giebt (1.)

$$39. \quad 0 = nu + r.$$

Also muſs r mit u *aufgehen* (§. 18.). Dieses geschieht nur dann, wenn $r = 0$ ist, indem r jedenfalls $< u$ sein soll. Also ist für $m = 0$, $r = 0$, und folglich vermöge (39.) auch $n = 0$.

Ist $r = 0$, so giebt (1.)

$$40. \quad mv = nu,$$

also muſs m mit u *aufgehen* (§. 25.). Dieses ist nur möglich, wenn $m = 0$ ist, indem $m < u$ sein soll. Also ist für $r = 0$, $m = 0$, und folglich vermöge (40.) auch $n = 0$.

So behauptet es (I.).

D. Setzt man (5., 6. und 4.) in (1.), so ergiebt sich

$$(\lambda u + m_0)v = (\lambda v + n_0 - \varepsilon)u + \varepsilon u + r_0 \quad \text{oder}$$

$$41. \quad m_0 v = n_0 u + r_0.$$

Diese Gleichung entspricht der (1.) mit allen den Werthen (7.) von m_0, (8.) von n_0 und (3.) von r_0. Also thun alle die durch (5. u. 6.) ausgedrückten Werthe von m und n mit jedem *beliebigen* λ der Gleichung (1.) ein Genüge; wie es (II.) behauptet.

E. Gäbe es noch andere Werthe von m und n, als die, welche (5. u. 6.) ausdrückt, so könnten es nur solche sein, die durch

$$42. \quad m = \lambda u + m_0 + \mu \quad \text{und}$$

$$43. \quad n = \lambda v + n_0 - \varepsilon + \nu$$

ausgedrückt werden, wo μ eine Zahl ist, die *nicht* mit u, ν eine Zahl, die *nicht* mit v *aufgeht;* denn ginge μ mit u auf, so wäre (42.) schon in (5.) und (43.) schon in (6.) *mitbegriffen,* indem dort λ *willkürlich* ist. Setzt man nun (42. u. 43.) nebst (4.) in (1.), so ergiebt sich

$$(\lambda u + m_0 + \mu)u = (\lambda v + n_0 - \varepsilon + \nu)u + \varepsilon u + r_0 \quad \text{oder}$$

$$44. \quad m_0 v + \mu v = n_0 u + \nu u + r_0.$$

Hiervon die Gleichung (41.), die nothwendig zugleich Statt findet, abgezogen, giebt

$$45. \quad \mu v = \nu u.$$

Dieses ist wieder nur möglich, wenn μ mit u und ν mit v *aufgeht* (§. 25.). Und da dies *nicht* sein *soll,* so finden die Ausdrücke (42. u. 43.) von m und

n nicht Statt: mithin giebt es aufser den Werthen von m und n, welche (5. u. 6.) ausdrückt, *keine andern;* wie es (II.) behauptet.

F. Da λ in (5. u. 6.) willkürlich ist, so kann es auch 0 und -1 sein. Dieses giebt

$$46.\quad m = m_0 \quad \text{und} \quad m = m_0 - u \quad \text{und}$$

$$47.\quad n = n_0 - \varepsilon \quad \text{und} \quad n = n_0 - \varepsilon - v.$$

Hier sind m_0 und $m_0 - u$ dieselben beiden m, (an zeichenfreien Werth beide $< u$) welche der Gleichung (1.) für Reste $< u$ genugthun. Also thun *dieselben beiden m* auch der Gleichung (1.) für *beliebige* Reste r (4.) genug. Dagegen sind die *zugehörigen* beiden Werthe $n_0 - \varepsilon$ und $n_0 - \varepsilon - v$ von n *nicht* nothwendig $< v$. Sie sind es nur, wenn $\varepsilon = 0$, also r eine der Zahlen (3.) ist.

Dieses ist, was (III.) behauptet.

G. Multiplicirt man die in (IV.) vorausgesetzte Gleichung

$$48.\quad m_1 v = n_1 u + 1$$

mit r, so ergiebt sich

$$49.\quad m_1 r v = n_1 r u + r.$$

Hiervon die Gleichung

$$50.\quad m_0 v = (n_0 - \varepsilon) u + r,$$

die sich ergiebt, wenn man (5. u. 6.) in (1.) und das willkürliche $\lambda = 0$ setzt, abgezogen, giebt

$$51.\quad (m_1 r - m_0) v = (n_1 r - (n_0 - \varepsilon)) u.$$

Dieser Gleichung gemäfs mufs $m_1 r - m_0$ mit u aufgehen (§. 25.) und also

$$52.\quad m_1 r - m_0 = \tau u$$

sein, wo τ irgend eine *ganze* Zahl ist. Ferner giebt (52.), in (51.) gesetzt,

$$\tau u v = (n_1 r - (n_0 - \varepsilon)) u, \text{ also}$$

$$53.\quad \tau v = n_1 r - (n_0 - \varepsilon).$$

Aus (52. u. 53.) folgt (10. u. 11.) zunächst für ein *positives* $m_0 < u$, und dann, wenn man noch u und v abzieht, also $\tau + 1$ statt τ schreibt, auch für ein negatives m_0, dessen absoluter Werth $< u$ ist.

Dies ist, was (IV.) behauptet.

H. Anm. Ein Hauptpunct des Beweises ist das Mittel, durch welches in (*A.*) gezeigt wird, dafs nicht zwei verschiedene Vielfachen von v zu u *gleiche* Reste lassen können. Es kommt sehr häufig zur Anwendung. Dann der Schlufs, dafs die Reste, weil sie alle verschieden und $> v$ und $< u$ sind, die Zahlen 1, 2, 3, 4, ... $u - 1$ selbst sein müssen. Auch dieser Schlufs kommt öfter vor.

§. 35.

Lehrsatz.

Es seien u *und* v *zwei beliebige zu einander* ***theilerfremde positive ganze*** *Zahlen.*

Setzt man in der Gleichung

$$1.\quad mv = \mathfrak{G}u + r$$

der Reihe nach

$$2.\quad m = 1, 2, 3, 4, \ldots \tfrac{1}{2}(u-1), \text{ wenn } u \text{ ungerade, und}$$

$$3.\quad m = 1, 2, 3, 4, \ldots \tfrac{1}{2}u, \text{ wenn } u \text{ gerade ist,}$$

und bezeichnet diejenigen Werthe von m, *welche in* (1.) ***positive Reste*** $r > \frac{1}{2}u$ *geben, durch* $m_1, m_2, m_3, \ldots m_\varkappa$, *die übrigen Werthe von* m, *welche positive Reste* ***nicht*** $> \frac{1}{2}u$ ***geben,*** *durch* $\mu_1, \mu_2, \mu_3, \ldots \mu_{\frac{1}{2}(u-1)-\varkappa}$ *oder* $\mu_{\frac{1}{2}u-\varkappa}$, *setzt darauf für alle* r, *die* $> \frac{1}{2}u$ *sind,*

$$4.\quad r = u - \varrho,$$

wo nun also auch alle ϱ, *eben wie die übrigen* r, ***nicht größer*** *als* $\frac{1}{2}u$ *sind, so dafs zusammengenommen*

Erstlich für ein ungerades u:

$$5.\ \begin{cases} m_1 v = \mathfrak{G}u + r_1, \\ m_2 v = \mathfrak{G}u + r_2, \\ m_3 v = \mathfrak{G}u + r_3, \\ \ldots\ldots\ldots\ldots \\ m_{\frac{1}{2}(u-1)-\varkappa} v = \mathfrak{G}u + r_{\frac{1}{2}(u-1)-\varkappa} \end{cases} \quad \text{und} \quad 6.\ \begin{cases} \mu_1 v = \mathfrak{G}u - \varrho_1, \\ \mu_2 v = \mathfrak{G}u - \varrho_2, \\ \mu_3 v = \mathfrak{G}u - \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \mu_\varkappa v = \mathfrak{G}u - \varrho_\varkappa; \end{cases}$$

Zweitens für ein gerades u:

$$7.\ \begin{cases} m_1 v = \mathfrak{G}u + r_1, \\ m_2 v = \mathfrak{G}u + r_2, \\ m_3 v = \mathfrak{G}u + r_3, \\ \ldots\ldots\ldots\ldots \\ m_{\frac{1}{2}u-\varkappa} v = \mathfrak{G}u + r_{\frac{1}{2}u-\varkappa} \end{cases} \quad \text{und} \quad 8.\ \begin{cases} \mu_1 v = \mathfrak{G}u - \varrho_1, \\ \mu_2 v = \mathfrak{G}u - \varrho_2, \\ \mu_3 v = \mathfrak{G}u - \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \mu_\varkappa v = \mathfrak{G}u - \varrho_\varkappa \end{cases}$$

ist, so sind die absoluten Werthe der r *und* ϱ ***zusammengenommen*** *nothwendig*

9. *Im ersten Falle* (5. u. 6.) *alle die Zahlen* $1, 2, 3, 4, \ldots \frac{1}{2}(u-1)$ und
10. *Im zweiten Falle* (7. u. 8.) *alle die Zahlen* $1, 2, 3, 4, \ldots \frac{1}{2}u$.

Beispiele. 1. Es sei

$$11.\quad u = 15, \quad v = 22,$$

so ist

12. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{S}u + 7, 14, 6, 13, 5, 12$ und 4.

Von diesen Resten sind die $\varkappa = 3$ Reste, 14, 13 und $12 > \frac{1}{2}u$, also ist in (5. u. 6.)

13. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{S}u + 7, -1, +6, -2, +5, -3$ und $+4$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäfs (9.).

2. Es sei

$$14. \quad u = 15, \quad v = 4,$$

so ist

15. $(1, 2, 3, 4, 5, 6, 7)v = Nu + 4, 8, 12, 1, 5, 9$ und 13.

Von diesen Resten sind die $\varkappa = 4$ Reste 8, 12, 9 und $13 > \frac{1}{2}u$, also ist in (5. und 6.)

16. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{S}u + 4, -7, -3, +1, +5, -6$ und -2.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäfs (9.).

3. Es sei

$$17. \quad u = 18, \quad v = 49,$$

so ist

18. $(1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{S}u + 13, 8, 3, 16, 11, 6, 1, 14$ und 9.

Von diesen Resten sind die $\varkappa = 4$ Reste 13, 16, 11 und $14 > \frac{1}{2}u$, also ist in (7. u. 8.)

19. $(1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{S}u - 5, +8, +3, -2, -7, +6, +1, -4$ und $+9$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 3, 4, 5, 6, 7, 8, 9; gemäfs (10.).

4. Es sei

$$20 \quad u = 22, \quad v = 15,$$

so ist

21. $(1, 2, 3, \ldots\ldots 11)v = \mathfrak{S}u + 15, 8, 1, 16, 9, 2, 17, 10, 3, 18, 11$.

Von diesen Resten sind die $\varkappa = 4$ Reste 15, 16, 17 und $18 > \frac{1}{2}u$, also ist in (7. u. 8.)

22. $(1, 2, 3, \ldots\ldots 11)v = \mathfrak{S}u - 7, +8, +1, -6, +9, +2, -5, +10, +3, -4, +11$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 und 11; gemäfs (10.).

Beweis. *A.* Kein r in (1.) kann $=0$ sein. Denn für $r=0$ wäre in (1.) $mv = \mathfrak{G}u$, also müfste m mit u aufgehen, da v zu u *theilerfremd* sein soll (§. 25.). m geht aber nicht mit u auf, weil alle $m < u$ sind (2. u. 3.); also kann r nicht $=0$ sein.

B. Wäre in (5. oder 7.) irgend ein r einem andern gleich, also z. B.

23. $m_\varepsilon v = \mathfrak{G}u + r$ und $m_\lambda v = \mathfrak{G}u + r$,

so würde daraus

24. $(m_\varepsilon - m_\lambda)v = \mathfrak{G}u$

folgen, und also müfste $m_\varepsilon - m_\lambda$ mit u aufgehen (§. 25.). Dieses ist aber nicht der Fall, da m_ε und m_λ beide $< u$ sind und also $m_\varepsilon - m_\lambda$ noch um so mehr $< u$ ist. Daher kann *kein r dem andern gleich sein.*

C. Ganz aus *gleichen* Gründen kann in (6. oder 8.) kein ϱ dem andern gleich sein.

D. Wäre in (5. und 6.) oder in (7. und 8.) ein r einem ϱ gleich, also z. B.:

25. $m_\varepsilon v = \mathfrak{G}u + r$ und $\mu_\lambda v = \mathfrak{G}u + r$

so würde daraus

26. $(m_\varepsilon + \mu_\lambda)v = \mathfrak{G}u$

folgen; also müfste $m_\varepsilon + \mu_\lambda$ mit u aufgehen (§. 25.). Aber in (5. und 6.) sind *alle* m oder $\mu < \frac{1}{2}u$ (2.) und in (7. und 8.) kann *nur eines* der m oder $\mu = \frac{1}{2}u$ sein (3.), die andern sind nothwendig *kleiner:* folglich ist *immer* $m_\varepsilon + \mu_\lambda < u$. Mithin kann $m_\varepsilon + \mu_\lambda$ *nicht* mit u aufgehen, und folglich kann in (5. und 6.), eben wie (7. und 8.), *kein r einem ϱ gleich sein.* Die r und ϱ sind also *alle* unter einander verschieden, und keins ist 0.

E. Nun ist die *Anzahl* der r und ϱ zusammengenommen der der m *gleich,* also in (5. und 6.) $= \frac{1}{2}(u-1)$ (2.) und in (7. und 8.) $= \frac{1}{2}u$ (3.): keins ist gröfser als $\frac{1}{2}u$, und alle sind von einander verschieden (*B.*, *C.* und *D.*). Also sind die r und ϱ zusammengenommen in (5. und 6.) nothwendig die Zahlen $1, 2, 3, \ldots \frac{1}{2}(u-1)$, und in (7. und 8.) nothwendig die Zahlen $1, 2, 3, \ldots \frac{1}{2}u$ selbst; wie es der Lehrsatz in (9. und 10.) behauptet.

F. Anm. Die in der Anmerkung zum vorigen Parapraph erwähnten Schlüsse sind auch hier die Hauptmomente des Beweises.

§. 36.

Lehrsatz.

Es seien u *und* v *zwei beliebige ungerade und zu einander theilerfremde ganze Zahlen und* z *sei eine beliebige positive ganze Zahl*

1. $z < \frac{1}{2}uv$.

Alsdann können, wenn man für ***ein und dasselbe*** z,

$$2.\quad z = m_1 u + r \quad \textit{und}$$

$$3.\quad z = m_2 v + \varrho$$

setzt, wo r *und* ϱ *die* ***echten positiven Reste*** *zu* u *und* v *bezeichnen, so daſs immer*

$$4.\quad r < u \quad \textit{und} \quad \varrho < v$$

ist, folgende verschiedene Fälle stattfinden.

5.
Erstlich, *wenn* $r > \frac{1}{2}u$ *ist, kann*
1) $\varrho = 0$,
2) $\varrho < \frac{1}{2}v > 0$,
3) $\varrho > \frac{1}{2}v$ *sein.*
Zweitens, *wenn* $r < \frac{1}{2}u > 0$ *ist, kann*
1) $\varrho = 0$,
2) $\varrho < \frac{1}{2}v > 0$ *und*
3) $\varrho > \frac{1}{2}v$ *sein.*
Drittens, *wenn* $r = 0$ *ist, kann*
1) $\varrho < \frac{1}{2}v > 0$ *und*
2) $\varrho > \frac{1}{2}v$ *sein.*

Bezeichnet man für diese 8 Fälle die ***Anzahl*** *der* $z < \frac{1}{2}uv$,

6.

1)	*für welche*	$r > \frac{1}{2}u$	*und*	$\varrho = 0$	*ist, durch*	n_1,
2)	- - -	$r > \frac{1}{2}u$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_2,
3)	- - -	$r > \frac{1}{2}u$	-	$\varrho > \frac{1}{2}v$	- - -	n_3,
4)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho = 0$	- - -	n_4,
5)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_5,
6)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho > \frac{1}{2}v$	- - -	n_6,
7)	- - -	$r = 0$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_7,
8)	- - -	$r = 0$	-	$\varrho > \frac{1}{2}v$	- - -	n_8,

so ist

Erstlich, *die* ***Gesammtheit*** *aller dieser verschiedenen* z,

$$7.\quad n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \tfrac{1}{2}(uv - 1).$$

Zweitens, *die Anzahl der* $n_7 + n_8$ *mit* u ***aufgehenden*** z *ist*

$$8.\quad n_7 + n_8 = \tfrac{1}{2}(v - 1).$$

Drittens, *die Anzahl der* $n_1 + n_4$ *mit* v ***aufgehenden*** z *ist*

$$9.\quad n_1 + n_4 = \tfrac{1}{2}(u - 1).$$

Viertens, *die Anzahl der* $n_2+n_5+n_7$ *verschiedenen* z, *welche, mit* v *dividirt, Reste* $\varrho<\frac{1}{2}v>0$ *lassen, gleichviel welche Reste* r *sie mit* u *dividirt geben mögen, ist*

$$10.\quad n_2+n_5+n_7=\tfrac{1}{4}(u+1)(v-1).$$

Fünftens, *die Anzahl der* $n_4+n_5+n_6$ *verschiedenen* z, *welche, mit* u *dividirt, Reste* $r<\frac{1}{2}u>0$ *lassen, gleichviel welche Reste* ϱ *sie mit* v *dividirt geben mögen, ist*

$$11.\quad n_4+n_5+n_6=\tfrac{1}{4}(u-1)(v+1).$$

Sechstens, *die Anzahl der* $n_3+n_6+n_8$ *verschiedenen* z, *welche, mit* v *dividirt, Reste* $\varrho>\frac{1}{2}v$ *lassen, gleichviel welche Reste* r *sie mit* u *dividirt geben mögen, ist*

$$12.\quad n_3+n_6+n_8=\tfrac{1}{4}(u-1)(v-1).$$

Siebentens, *die Anzahl der* $n_1+n_2+n_3$ *verschiedenen* z, *welche mit* u *dividirt Reste* $r>\frac{1}{2}u$ *lassen, gleichviel welche Reste* ϱ *sie mit* v *dividirt geben mögen, ist*

$$13.\quad n_1+n_2+n_3=\tfrac{1}{4}(u-1)(v-1).$$

Achtens, *die Anzahl der* n_3+n_5 *verschiedenen* z, *welche mit* u *und mit* v *dividirt entweder* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\varrho>\frac{1}{2}v$, *oder* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\varrho<\frac{1}{2}v>0$ *lassen, ist*

$$14.\quad n_3+n_5=\tfrac{1}{4}(u-1)(v-1).$$

Neuntens, *die Anzahl der* n_2+n_6 *verschiedenen* z, *welche mit* u *und mit* v *dividirt entweder* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\varrho<\frac{1}{2}v>0$, *oder* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\varrho>\frac{1}{2}v$ *lassen, ist*

$$15.\quad n_2+n_6=\tfrac{1}{4}(u-1)(v-1).$$

Zehntens, *die* ***doppelte*** *Anzahl* $2n_5$ *derjenigen* z, *welche mit* u *und mit* v *dividirt* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\varrho<\frac{1}{2}v>0$ *lassen, weniger der Anzahl* n_1 *derjenigen mit* v ***aufgehenden*** z, *welche mit* u *dividirt Reste* $>\frac{1}{2}u$ *lassen, und der mit* u ***aufgehenden*** n_8 *Zahlen* z, *welche mit* v *dividirt Reste* $>\frac{1}{2}v$ *lassen, ist*

$$16.\quad 2n_5-n_1-n_8=\tfrac{1}{4}(u-1)(v-1).$$

Elftens, *die Anzahl der mit* v ***aufgehenden*** n_1 *verschiedenen* z, *welche Reste* $>\frac{1}{2}u$ *lassen, zusammen mit der Anzahl der* n_8 *mit* u ***aufgehenden*** z, *welche Reste* $>\frac{1}{2}v$ *lassen, und der Anzahl* n_3 *der* z, *welche mit* u *und* v *dividirt* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\varrho>\frac{1}{2}v$ *lassen, ist der Anzahl* n_5 *derjenigen* z ***gleich***, *welche mit* u *und* v *dividirt zugleich Reste* $r<\frac{1}{2}u>0$ *und* $\varrho<\frac{1}{2}v>0$ *lassen,*

das heifst, es ist

17. $n_1 + n_8 + n_3 = n_5$.

Beispiel. Es sei

18. $u = 7$, $v = 11$, also $uv = 77$ und

19. $z = 1, 2, 3, 4, \ldots 38 (= \frac{1}{2}(uv - 1))$,

so geben die beiden Gleichungen (2. u. 3.) Folgendes:

20.

Für $z =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ist $m_1 =$	0	0	0	0	0	0	1	1	1	1	1	1	1	2	2	2	2	2	2
$r =$	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5
$m_2 =$	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
$\varrho =$	1	2	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
21.	5	5	5	2	2	3	8	6	6	6	1	2	2	7	5	5	6	3	3

Für $z =$	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
ist $m_1 =$	2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5	5	5
$r =$	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3
$m_2 =$	1	1	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3
$\varrho =$	9	10	0	1	2	3	4	5	6	7	8	9	10	0	1	2	3	4	5
21.	3	8	4	5	5	2	2	2	8	6	6	6	3	1	2	7	5	5	5

Die horizontale Zeile (21.) giebt die *Nummer* der 8 Classen (6.) an, in welche jedes z gehört. Z. B.: Für $z = 17$ ist $r = 3 < \frac{1}{2}u > 0$ und $\varrho = 6 > \frac{1}{2}v$, also gehört $z = 17$ in die *sechste* Classe (6.); und so die andern. Zufolge (21.) gehören also

22.
- die 2 Zahlen 11 und 33 in die *erste* Classe, folglich ist hier $n_1 = 2$;
- die 8 Zahlen 4, 5, 12, 13, 25, 26, 27 und 34 gehören in die *zweite* Classe, also ist $n_2 = 8$;
- die 5 Zahlen 6, 18, 19, 20 und 32 gehören in die *dritte* Classe, also ist $n_3 = 5$;
- die 1 Zahl 22 gehört in die *vierte* Classe, also ist . . $n_4 = 1$;
- die 10 Zahlen 1, 2, 3, 15, 16, 23, 24, 36, 37 und 38 gehören in die *fünfte* Classe, also ist $n_5 = 10$;
- die 7 Zahlen 8, 9, 10, 17, 29, 30, 31 gehören in die *sechste* Classe, also ist $n_6 = 7$;
- die 2 Zahlen 14 und 35 gehören in die *siebente* Classe, also ist $n_7 = 2$;
- die 3 Zahlen 7, 21 und 28 gehören in die *achte* Classe, also ist $n_8 = 3$.

Diese Werthe der verschiedenen n thun nun wie folgt den Gleichungen (7. bis 17.) des Lehrsatzes Genüge. Nemlich

23.
- die Gleichung (7.) ist hier $2+8+5+1+10+7+2+3 = 38 = \frac{1}{2}(uv-1)$,
- - - - (8.) - - $2+3 = 5 = \frac{1}{2}(v-1)$,
- - - - (9.) - - $2+1 = 3 = \frac{1}{2}(u-1)$,
- - - - (10.) - - $8+10+2 = 20 = \frac{1}{4}(u+1)(v-1) = \frac{1}{4}.8.10$,

$$23.\quad \begin{cases} \text{die Gleichung (11.) ist hier } 1+10+7=18=\frac{1}{4}(u-1)(v+1)=\frac{1}{4}.6.12, \\ \text{- - - (12.) - - } 5+7+3=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ \text{- - - (13.) - - } 2+8+5=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ \text{- - - (14.) - - } 5+10=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ \text{- - - (15.) - - } 8+7=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ \text{- - - (16.) - - } 2.10-2-3=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ \text{- - - (17.) - - } 2+3+5=10; \end{cases}$$

Alles wie gehörig.

Beweis. *A*. Dafs alle die 8 verschiedenen Classen für die z stattfinden *können*, ist offenbar. Es ist nur zu bemerken, dafs nicht, wie es scheinen könnte, auch noch für (5. Drittens), eben wie (5. Erstlich und Zweitens), ein *dritter* Fall $r=0$ und *zugleich* $\varrho=0$, also keine *neunte* Classe möglich ist. Denn könnte ein z mit u und v *zugleich aufgehen*, so würde es, da u und v nach der Voraussetzung zu einander *theilerfremd* sind, zufolge (§. 26.) auch mit dem Product uv *aufgehen* müssen; was nicht möglich ist, da das *gröfste* der z erst $\frac{1}{2}(uv-1)$ ist und also *alle* $z<uv$ sind.

B. Dafs kein z in *mehr als einer* Classe *zugleich* vorkommen kann, ist ebenfalls offenbar; denn eine Zahl z kann zu einer andern u oder v nicht *verschiedene* Reste zugleich lassen. Da nun zugleich jedes z nothwendig in einer der 8 Classen vorkommen *mufs*, indem nicht mehr als die 8 Fälle möglich sind, so folgt, dafs die *Summe* der Mengen der z in den verschiedenen 8 Classen der Anzahl der z *selbst* gleich ist. Diese letztere ist $\frac{1}{2}(uv-1)$, also mufs

$$24.\quad n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8 = \tfrac{1}{2}(uv-1)$$

sein. Dies ist die Gleichung (7.) des Lehrsatzes.

C. Die mit u *aufgehenden* z, n_7+n_8 an der Zahl, sind offenbar die *Vielfachen*

$$25.\quad u,\ 2u,\ 3u,\ 4u,\ \ldots\ \tfrac{1}{2}(v-1)u$$

von u, und keine mehr; denn das *nächste* Vielfache von u, nemlich $\frac{1}{2}(v+1)u$, ist schon *gröfser* als der *gröfste* Werth $\frac{1}{2}(uv-1)$ von z. Die Anzahl jener Vielfachen von u (25.) ist aber $\frac{1}{2}(v-1)$, also ist

$$26.\quad n_7+n_8 = \tfrac{1}{2}(v-1).$$

Dieses ist die Gleichung (8.) des Lehrsatzes.

D. Die mit v *aufgehenden* z, n_1+n_4 an der Zahl, sind die *Vielfachen*

$$27.\quad v,\ 2v,\ 3v,\ 4v,\ \ldots\ \tfrac{1}{2}(u-1)v$$

von v, und keine mehr; denn das *nächste* Vielfache von v, nemlich $\frac{1}{2}(u+1)v$, ist schon *gröfser* als der *gröfste* Werth $\frac{1}{2}(uv-1)$ von z. Die Anzahl der

Vielfachen von v (27.) ist aber $\frac{1}{2}(u-1)$, also ist

$$28.\quad n_1+n_4=\tfrac{1}{2}(u-1).$$

Dieses ist die Gleichung (9.) des Lehrsatzes.

E. Folgende Zahlen z, und keine anderen, nemlich:

29. Die $\frac{1}{2}(u+1)$ Zahlen $1,\ v+1,\ 2v+1,\ 3v+1,\ \dots\ \frac{1}{2}(u-1)v+1$ lassen zu v den Rest 1,
Die $\frac{1}{2}(u+1)$ Zahlen $2,\ v+2,\ 2v+2,\ 3v+2,\ \dots\ \frac{1}{2}(u-1)v+2$ lassen zu v den Rest 2,
Die $\frac{1}{2}(u+1)$ Zahlen $3,\ v+3,\ 2v+3,\ 3v+3,\ \dots\ \frac{1}{2}(u-1)v+3$ lassen zu v den Rest 3,
. .
Die $\frac{1}{2}(u+1)$ Zahlen $\frac{1}{2}(v-1),\ v+\frac{1}{2}(v-1),\ 2v+\frac{1}{2}(v-1),\ \dots\ \frac{1}{2}(u-1)v+\frac{1}{2}(v-1)$ lassen zu v den Rest $\frac{1}{2}(v-1)$.

Alle diese Zahlen finden sich unter den Werthen, welche z haben kann; denn die *gröfste* unter ihnen $\frac{1}{2}(u-1)v+\frac{1}{2}(v-1)=\frac{1}{2}(uv-1)$ ist nur eben so grofs als z soll sein können; alle andern sind kleiner. Desgleichen lassen sie *alle* zu v Reste, die $<\frac{1}{2}v$ und >0 sind. Sie sind also zusammengenommen die $n_2+n_5+n_7$ Zahlen z in der 2ten, 5ten und 7ten Classe (6.).

Nun ist die Anzahl der z in (29.) $=\frac{1}{2}(u+1).\frac{1}{2}(v-1)$, denn in jeder horizontalen Reihe stehen $\frac{1}{2}(u+1)$ Zahlen und die Anzahl der Reihe ist $\frac{1}{2}(v-1)$. Also ist

$$30.\quad n_2+n_5+n_7=\tfrac{1}{4}(u+1)\tfrac{1}{2}(v-1).$$

Dieses ist die Gleichung (10.) des Lehrsatzes.

F. Folgende Zahlen z, und keine anderen, nemlich:

31. Die $\frac{1}{2}(v+1)$ Zahlen $1,\ u+1,\ 2u+1,\ 3u+1,\ \dots\ \frac{1}{2}(v-1)u+1$ lassen zu u den Rest 1,
Die $\frac{1}{2}(v+1)$ Zahlen $2,\ u+2,\ 2u+2,\ 3u+2,\ \dots\ \frac{1}{2}(v-1)u+2$ lassen zu u den Rest 2,
Die $\frac{1}{2}(v+1)$ Zahlen $3,\ u+3,\ 2u+3,\ 3u+3,\ \dots\ \frac{1}{2}(v-1)u+3$ lassen zu u den Rest 3,
. .
Die $\frac{1}{2}(v+1)$ Zahlen $\frac{1}{2}(u-1),\ u+\frac{1}{2}(u-1),\ 2u+\frac{1}{2}(u-1),\ \dots\ \frac{1}{2}(v-1)u+\frac{1}{2}(u-1)$ lassen zu u den Rest $\frac{1}{2}(u-1)$.

Alle diese Zahlen finden sich unter den Werthen, welche z haben kann; denn die *gröfste* unter ihnen ist $\frac{1}{2}(v-1)u+\frac{1}{2}(u-1)=\frac{1}{2}(uv-1)$, also nur das gröfste z. Alle andern sind kleiner. Auch lassen sie *alle* zu u Reste, die $<\frac{1}{2}u$ und >0 sind. Sie sind also zusammen die $n_4+n_5+n_6$ Zahlen z in der 4ten, 5ten und 6ten Classe (6.).

Die Anzahl der z in (31.) ist aber $\frac{1}{2}(v+1).\frac{1}{2}(u-1)$, denn jede der $\frac{1}{2}(u-1)$ horizontalen Reihen enthält $\frac{1}{2}(v+1)$ Zahlen. Also ist

$$32.\quad n_4+n_5+n_6=\tfrac{1}{4}(u-1)(v+1).$$

Dieses ist die Gleichung (11.) des Lehrsatzes.

G. Die $n_3+n_6+n_8$ Zahlen z in (6.) lassen sämmtlich nach v Reste $\varrho>\frac{1}{2}v$. Zieht man $n_1+n_4=\frac{1}{2}(u-1)$ (9.) und $n_2+n_5+n_7=\frac{1}{4}(u+1)(v-1)$ (10.) von $n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_3+n_6+n_8 = \tfrac{1}{2}(uv-1)-\tfrac{1}{2}(u-1)-\tfrac{1}{4}(u+1)(v-1) \text{ oder}$$
$$= \tfrac{1}{2}uv-\tfrac{1}{2}-\tfrac{1}{2}u+\tfrac{1}{2}-\tfrac{1}{4}uv+\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} \text{ oder}$$
$$33.\quad n_3+n_6+n_8 = \tfrac{1}{4}uv-\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dies ist die Gleichung (12.) des Lehrsatzes.

H. Die $n_1+n_2+n_3$ Zahlen z in (6.) lassen sämmtlich nach u Reste $r>\frac{1}{2}u$. Zieht man $n_7+n_8=\frac{1}{2}(v-1)$ (8.) und $n_4+n_5+n_6=\frac{1}{4}(u-1)(v+1)$ (11.) von $n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_1+n_2+n_3 = \tfrac{1}{2}(uv-1)-\tfrac{1}{2}(v-1)-\tfrac{1}{4}(u-1)(v+1) \text{ oder}$$
$$= \tfrac{1}{2}uv-\tfrac{1}{2}-\tfrac{1}{2}v+\tfrac{1}{2}-\tfrac{1}{4}uv-\tfrac{1}{4}u+\tfrac{1}{4}v+\tfrac{1}{4} \text{ oder}$$
$$34.\quad n_1+n_2+n_3 = \tfrac{1}{4}uv-\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dies ist die Gleichung (13.) des Lehrsatzes.

I. a. So wie die $\frac{1}{2}(uv-1)$ Zahlen

$$35.\quad 1,\ 2,\ 3,\ 4,\ \ldots\ \tfrac{1}{2}(uv-1)$$

durch z bezeichnet wurden, so mögen die *weiter folgenden* $\frac{1}{2}(uv-1)$ Zahlen

$$36.\quad \tfrac{1}{2}(uv+1),\quad \tfrac{1}{2}(uv+3),\quad \tfrac{1}{2}(uv+5),\ \ldots\ uv-1$$

durch w bezeichnet werden. Alsdann gehört zu *jedem* z ein w, und *nur ein* w, welches mit ihm zusammen uv ausmacht: nemlich 1 mit $uv-1$, 2 mit $uv-2$, 3 mit $uv-3$, ... $\frac{1}{2}(uv-1)$ mit $\frac{1}{2}(uv+1)$ zusammen machen sämmtlich uv aus. Wenn man also in der Gleichung

$$37.\quad z+w=uv$$

dem z *alle* die $\frac{1}{2}(uv-1)$ Werthe (35.), die es haben kann, giebt, so hat w seinerseits *alle* die $\frac{1}{2}(uv-1)$ Werthe (36.), die ihm zukommen.

b. Nun sei für irgend ein z, welches weder mit u noch mit v *aufgeht*, nach (2. u. 3.)

$$38.\quad z=m_1u+r=m_2v+\varrho,$$

wo also weder r noch ϱ Null aber $r<u$, $\varrho<v$ ist. Für das *zugehörige* w sei

$$39.\quad w=\mu_1u+r'=\mu_2v+\varrho',$$

wo $r'<u$ und $\varrho'<v$ angenommen wird; alsdann kann auch weder r' noch ϱ' Null sein. Denn ginge w mit u oder mit v auf, so müfste zufolge (37.) auch z mit u oder mit v aufgehen, gegen die Voraussetzung. Zufolge (37.) ist aus (38. u. 39.)

$$40.\quad z+w=(m_1+\mu_1)u+r+r'=(m_2+\mu_2)v+\varrho+\varrho'=uv.$$

Dieses ist so viel als die *zwei* Gleichungen

$$41.\quad uv=(m_1+\mu_1)u+r+r' \text{ und}$$
$$42.\quad uv=(m_2+\mu_2)v+\varrho+\varrho'.$$

Aus (41. u. 42.) folgt, dafs $r+r'$ mit u und $\varrho+\varrho'$ mit v *aufgehen* mufs (§. 18.). Aber $r+r'$ ist >0 und $<2u$, weil $r>0<u$ und $r'>0<u$; also mufs nothwendig

$$43.\quad r+r'=u$$

sein; denn zwischen 0 und $2u$ liegt keine andere Zahl als u selbst, die mit u aufginge. Gleichmäfsig ist $\varrho+\varrho'>0$ und $<2v$, weil $\varrho>0<v$ und $\varrho'>0<v$ ist; also mufs auch nothwendig

$$44.\quad \varrho+\varrho'=v$$

sein; aus gleichen Gründen.

Aus (43. u. 44.) folgt nun weiter, dafs, wenn $r>\frac{1}{2}u$ ist, $r'<\frac{1}{2}u>0$ sein mufs, und umgekehrt; desgleichen, dafs, wenn $\varrho>\frac{1}{2}v$ ist, $\varrho'<\frac{1}{2}v>0$ sein mufs, und umgekehrt.

c. Nun sind n_3 Zahlen z vorhanden, für welche $r>\frac{1}{2}u$ und *zugleich* $\varrho>\frac{1}{2}v$ ist (6.), also mufs es *eben so viele* Zahlen w geben, für welche $r'<\frac{1}{2}u>0$ und *zugleich* $\varrho'<\frac{1}{2}v>0$ ist, denn zu jedem z gehört ein w, für welches $r'<\frac{1}{2}u>0$ und $\varrho'<\frac{1}{2}v>0$, wenn für das zugehörige z, $r>\frac{1}{2}u$ und $\varrho>\frac{1}{2}v$ ist (6.).

Desgleichen sind n_5 Zahlen z vorhanden, für welche $r<\frac{1}{2}u>0$ und *zugleich* $\varrho<\frac{1}{2}v>0$ ist (6.), also mufs es *eben so viele* Zahlen w geben, für welche $r'>u$ und *zugleich* $\varrho'>\frac{1}{2}v$ ist; aus gleichen Gründen.

Es sind also unter den Zahlen z und w *zusammengenommen*, das heifst unter den Zahlen

$$45.\quad 1,\ 2,\ 3,\ 4,\ \ldots\ uv-1$$

nothwendig überhaupt n_3+n_5 Zahlen vorhanden, die, weder mit u noch mit v *aufgehend*, nach u Reste r oder $r'>\frac{1}{2}u$ und *zugleich* nach v Reste ϱ *oder* $\varrho'>\frac{1}{2}v$ lassen; und *eben so viele* Zahlen, welche, weder mit u noch mit v *aufgehend*, nach u Reste r *oder* $r'<\frac{1}{2}u>0$ und *zugleich* nach v Reste ϱ *oder* $\varrho'<\frac{1}{2}v>0$ lassen.

d. Um durch u und v ausgedrückt zu finden, wie viele solcher letztgenannten Zahlen unter den z und w zusammengenommen sich befinden, bezeichne x jede derjenigen Zahlen aus der *Gesammtheit* der z und w, also aus den Zahlen (45.), welche mit u dividirt einen Rest $\varepsilon<\frac{1}{2}u>0$ und mit v dividirt einen Rest $\sigma<\frac{1}{2}v>0$ läfst; so dafs also

$$46.\quad x=eu+\varepsilon=sv+\sigma$$

ist, wo $\varepsilon<\frac{1}{2}u>0$, *zugleich* $\sigma<\frac{1}{2}v>0$ und $x<uv$ also $e<v$, $s<u$ sein soll.

e. Aus (46.) folgt

$$47. \quad sv = eu + \varepsilon - \sigma.$$

In dieser Gleichung soll also ε alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ bekommen können, während $s<u$, $e<v$ ist. Was nun auch $\varepsilon-\sigma$ sein mag, positiv, oder negativ, oder Null: immer giebt es nach (§. 34. III.) einen Werth von $s<u$, welcher der Gleichung (47.) genug thut; also kann in (47.) und folglich in (46.) in der That $s<u$ und folglich, da σ nothwendig $<v$ ist, auch $x<uv$ sein. Also kann in (46.) ε wirklich alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ haben, für $x<uv$.

f. Nun kann zunächst in (46.) erst ε ohne Rücksicht auf $sv+\sigma$ offenbar alle die Werthe $1, 2, 3, 4, \ldots \frac{1}{2}(u-1)$ haben; denn *alle* die x, welche diese Werthe des Restes ε geben, sind *vorhanden*.

Aber giebt man dem ε irgend einen *bestimmten* Werth, z. B. 1, so kann zufolge (*e.*) für dieses *nemliche* $\varepsilon=1$, σ jeden der $\frac{1}{2}(v-1)$ Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ haben, und zwar offenbar immer für ein *anderes* x, da ein und dasselbe x nicht verschiedene Reste σ lassen kann. Für $\varepsilon=1$ findet sich also zu jedem $\sigma=1, 2, 3, \ldots \frac{1}{2}(v-1)$ irgend ein x. Folglich giebt es in (46.) $\frac{1}{2}(v-1)$ *verschiedene* x, die alle den Rest $\varepsilon=1$, aber die *verschiedenen* Reste $\sigma=1, 2, 3, \ldots \frac{1}{2}(v-1)$ lassen.

Ganz gleich verhält es sich für *jeden* der $\frac{1}{2}(u-1)$ Werthe $1, 2, 3, \ldots \ldots \frac{1}{2}(u-1)$, welche ε haben kann.

Also giebt es überhaupt $\frac{1}{2}(u-1).\frac{1}{2}(v-1) = \frac{1}{4}(u-1)(v-1)$ verschiedene x unter den Zahlen (45.), welche nach u Reste $<\frac{1}{2}u>0$ und *zugleich* nach v Reste $<\frac{1}{2}v>0$ lassen. Die Anzahl dieser Zahlen war (*c.*) $=n_3+n_5$, also ist

$$48. \quad n_3+n_5 = \tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (14.) des Lehrsatzes.

K. Zieht man $n_7+n_8=\frac{1}{2}(v-1)$ (8.), $n_1+n_4=\frac{1}{2}(u-1)$ (9.) und $n_3+n_5=\frac{1}{4}(u-1)(v-1)$ (14.) von $n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_2+n_6 = \tfrac{1}{2}(uv-1)-\tfrac{1}{2}(v-1)-\tfrac{1}{2}(u-1)-\tfrac{1}{4}(u-1)(v-1) \text{ oder}$$

$$n_2+n_6 = \tfrac{1}{2}uv-\tfrac{1}{2}-\tfrac{1}{2}v+\tfrac{1}{2}-\tfrac{1}{2}u+\tfrac{1}{2}-\tfrac{1}{4}uv+\tfrac{1}{4}u+\tfrac{1}{4}v-\tfrac{1}{4} \text{ oder}$$

$$49. \quad n_2+n_6 = \tfrac{1}{4}uv-\tfrac{1}{2}u-\tfrac{1}{2}v+\tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (15.) des Lehrsatzes.

L. Addirt man $n_2+n_6=\frac{1}{4}(u-1)(v-1)$ (15.) zu $2(n_3+n_5)=\frac{1}{2}(u-1)(v-1)$ (14.) und zieht von der Summe $n_2+n_6+n_8=\frac{1}{4}(u-1)(v-1)$ (12.) und $n_1+n_2+n_3=\frac{1}{4}(u-1)(v-1)$ (13.) ab, so ergiebt sich $2(n_3+n_5)+n_2+n_6-n_3-n_6-n_8-n_1-n_2-n_3=(\frac{1}{2}+\frac{1}{4}-\frac{1}{4}-\frac{1}{4})(u-1)(v-1)$ oder

$$50.\quad 2n_5-n_1-n_8=\tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (16.) des Lehrsatzes.

M. Zieht man endlich $n_3+n_5=\frac{1}{4}(u-1)(v-1)$ (14.) von $2n_5-n_1-n_8=\frac{1}{4}(u-1)(v-1)$ (16.) ab, so ergiebt sich

$$2n_5-n_1-n_8-n_3-n_5=0 \text{ oder}$$

$$51.\quad n_1+n_8+n_3=n_5.$$

Dieses ist die Gleichung (17.) des Lehrsatzes.

N. Anm. Der Theil des Beweises (*I.*) enthält eigenthümliche Erwägungen und bedarf wesentlich des Satzes (§. 34.), welcher auch weiterhin oft nöthig ist. Alles Übrige ist sehr einfach.

§. 37.

Lehrsatz.

I. *Es seien* m *und* n *zwei beliebige positive ganze Zahlen und es sei*

$$1.\quad n > m.$$

Setzt man

$$2.\ \begin{cases} m = \mu_1 n + r_1, \\ 2m = \mu_2 n + r_2, \\ 3m = \mu_3 n + r_3, \\ \ldots\ldots\ldots \\ (n-1)m = \mu_{n-1} n + r_{n-1}, \\ nm = \mu_n\, n + r_n, \end{cases} \quad \textit{und}\quad 3.\ \begin{cases} n = \nu_1 m + \varrho_1, \\ 2n = \nu_2 m + \varrho_2, \\ 3n = \nu_3 m + \varrho_3, \\ \ldots\ldots\ldots \\ (m-1)n = \nu_{m-1} m + \varrho_{m-1}, \\ mn = \nu_m\, m + \varrho_m \end{cases}$$

unter der Bedingung, daſs die sämmtlichen r *und* ϱ *positiv sind und*

4. *die* r *aus den Zahlen* 1, 2, 3, 4, ... n,

5. *die* ϱ *aus den Zahlen* 0, 1, 2, 3, ... m—1

genommen werden, und bezeichnet die Summe der sämmtlichen Quotienten μ, *nemlich*

6. $\mu_1+\mu_2+\mu_3 \ldots\ldots + \mu_{n-1}+\mu_n$ *durch* $S\mu$;

die Summe der sämmtlichen Quotienten ν, *nemlich*

7. $\nu_1+\nu_2+\nu_3 \ldots\ldots + \nu_{m-1}+\nu_m$ *durch* $S\nu$;

die Summe der sämmtlichen Reste r, nemlich

8. $r_1+r_2+r_3 \ldots\ldots + r_{n-1}+r_n$ *durch* Sr;

die Summe der sämmtlichen Reste ϱ, *nemlich*

$$9.\quad \varrho_1+\varrho_2+\varrho_3\ldots\ldots+\varrho_{m-1}+\varrho_m \text{ durch } S\varrho,$$

so ist

$$10.\quad r_n=n,\quad \varrho_m=0,$$

$$11.\quad \mu_n=m-1 \text{ und } \nu_m=n,$$

$$12.\quad S\mu+S\nu=mn,$$

$$13.\quad mSr+nS\varrho=\tfrac{1}{2}mn(m+n).$$

II. *Sind* m *und* n *zu einander theilerfremd, so ist*

$$14.\quad Sr=\tfrac{1}{2}n(n+1),$$

$$15.\quad S\varrho=\tfrac{1}{2}m(m-1),$$

$$\left.\begin{array}{ll}16. & S\mu=\tfrac{1}{2}(n+1)(m-1)\\ 17. & S\nu=\tfrac{1}{2}((n-1)m+n+1)\end{array}\right\} S\mu+S\nu=mn,$$

$$18.\quad S\mu-\mu_n=S\nu-\nu_m=\tfrac{1}{2}(n-1)(m+1).$$

Beispiel 1. Es sei für *beliebige* m und n,

$$19.\quad m=8,\quad n=20,$$

so ist in (2 u. 3.)

$$20.\ \left\{\begin{array}{r}1,\ 2m=0n+8,\ 16,\\ 3,\ 4,\ 5m=1n+4,\ 12,\ 20,\\ 6,\ 7m=2n+8,\ 16,\\ 8,\ 9,\ 10m=3n+4,\ 12,\ 20,\\ 11,\ 12m=4n+8,\ 16,\\ 13,\ 14,\ 15m=5n+4,\ 12,\ 20,\\ 16,\ 17m=6n+8,\ 16,\\ 18,\ 19,\ 20m=7n+4,\ 12,\ 20,\end{array}\right. \quad \text{und}\quad 21.\ \left\{\begin{array}{l}1n=2m+4,\\ 2n=5m+0,\\ 3n=7m+4,\\ 4n=10m+0,\\ 5n=12m+4,\\ 6n=15m+0,\\ 7n=17m+4,\\ 8n=20m+0.\end{array}\right.$$

Die Summe *aller* Quotienten μ und ν ist hier

$$S\mu+S\nu=2.0+3.1+2.2+3.3+2.4+3.5+2.6+3.7+2+5+7+10+12+15+17+20, \text{ oder}$$

$$22.\quad S\mu+S\nu=3+4+9+8+15+12+21+88=160=8.20=mn;$$

gemäfs (12.). Ferner ist

$$23.\quad \mu_n=7=m-1 \text{ und } \nu_m=20=n; \text{ gemäfs (11.)},$$

$$24.\quad mSr+nS\varrho=8(8+16+4+12+20)4+20.4.4=4.8.60+320$$
$$=2240=\tfrac{1}{2}.8.20(8+20)=\tfrac{1}{2}mn(m+n); \text{ gemäfs (13.)},$$

$$25.\quad r_n=20=n \text{ und } \varrho_m=0; \text{ gemäfs (10.)}.$$

Beispiel 2. Es sei für *theilerfremde* m und n,

$$26.\quad m=9,\quad n=38,$$

so ist in (2. u. 3.)

$$27.\quad\left\{\begin{array}{l} 1,\ 2,\ 3,\ 4m = 0n+9,\ 18,\ 27,\ 36,\\ 5,\ 6,\ 7,\ 8m = 1n+7,\ 16,\ 25,\ 34,\\ 9,\ 10,\ 11,\ 12m = 2n+5,\ 14,\ 23,\ 32,\\ 13,\ 14,\ 15,\ 16m = 3n+3,\ 12,\ 21,\ 30,\\ 17,\ 18,\ 19,\ 20,\ 21m = 4n+1,\ 10,\ 19,\ 28,\ 37,\\ 22,\ 23,\ 24,\ 25m = 5n+8,\ 17,\ 26,\ 35,\\ 26,\ 27,\ 28,\ 29m = 6n+6,\ 15,\ 24,\ 33,\\ 30,\ 31,\ 32,\ 33m = 7n+4,\ 13,\ 22,\ 31,\\ 34,\ 35,\ 36,\ 37,\ 38m = 8n+2,\ 11,\ 20,\ 29,\ 38,\end{array}\right.\qquad 28.\quad\left\{\begin{array}{l} 1n = 4m+2,\\ 2n = 8m+4,\\ 3n = 12m+6,\\ 4n = 16m+8,\\ 5n = 21m+1,\\ 6n = 25m+3,\\ 7n = 29m+5,\\ 8n = 33m+7,\\ 9n = 38m+0.\end{array}\right.$$

Die Summe der Quotienten μ und ν ist hier

$$S\mu = 4.0+4.1+4.2+4.3+5.4+4.5+4.6+4.7+5.8 \text{ oder}$$

29. $S\mu = 4+8+12+20+20+24+28+40 = 156 = \frac{1}{2}(38+1)(9-1)$
$= \frac{1}{2}.39.8 = \frac{1}{2}(n+1)(m-1)$; gemäfs (16.).

Die Summe der Quotienten ν ist

30. $S\nu = 4+8+12+16+21+25+29+33+38 = 186$
$= \frac{1}{2}((38-1).9+38+1) = \frac{1}{2}(37.9+39) = 186 = \frac{1}{2}((n-1)m+n+1)$;

gemäfs (17.). Ferner ist

31. $S\mu - \mu_n = 156-8 = S\nu - \nu_m = 186-38 = 148 = \frac{1}{2}.37.8$
$= \frac{1}{2}(n-1)(m-1)$; gemäfs (18.),

32. $Sr = (1+2+3 \ldots + 38) = \frac{1}{2}.38.39 = \frac{1}{2}n(n+1)$; gemäfs (14.),

33. $S\varrho = (1+2+3 \ldots + 8) = \frac{1}{2}.8.9 = \frac{1}{2}m(m-1)$; gemäfs (15.).

Beweis. *A.* Da $m<n$ sein soll und zufolge der *ersten* Gleichung (3.) $\nu_1 m$ noch um ϱ_1 kleiner als n ist, so ist in (2.) für m, $2m$, $3m$, ... $\nu_1 m$ nothwendig $\mu_1 = 0$. Also sind die *ersten* ν_1 Quotienten μ_1, μ_2, μ_3, ... μ_{ν_1} sämmtlich Null.

Das nächstfolgende Vielfache $(\nu_1+1)m$ von m ist schon $>n$; denn, noch einmal m zu der ersten Gleichung (3.) gethan, würde einen Rest ϱ_1+m geben, der $>m$ wäre; was nicht sein soll. Also ist der Quotient μ_{ν_1+1} in (2.) der *erste* derjenigen, welche *nicht Null,* sondern 1 sind. Aber $\nu_2 m$ ist nach der 2ten Gleichung in (3.) noch um ϱ_2 kleiner als $2n$. Also sind in (2.) auch alle folgenden Vielfachen $(\nu_1+2)m$, $(\nu_1+3)m$, $(\nu_1+4)m$ etc., von m bis zu $\nu_2 m$, noch kleiner als $2n$, und folglich sind alle die $\nu_2-\nu_1$ Quotienten μ_{ν_1+1}, μ_{ν_1+2}, μ_{ν_1+3}, ... μ_{ν_2} in (2.) sämmtlich $= 1$.

Auf dieselbe Weise folgt, dafs die sämmtlichen $\nu_3-\nu_2$ Quotienten μ_{ν_2+1}, μ_{ν_2+2}, ν_{ν_2+3}, ... μ_{ν_3} in (2.) $= 2$ sind, die sämmtlichen $\nu_4-\nu_3$ Quo-

tienten μ_{ν_3+1}, μ_{ν_3+2}, μ_{ν_3+3}, ... μ_{ν_4} in (2.) = 3; u. s. w. Zuletzt also sind die letzten $\nu_m - \nu_{m-1}$ Quotienten μ gleich $m-1$.

B. Nimmt man dieses zusammen, so ergiebt sich Folgendes:

34. $$\begin{cases} \text{die ersten } \nu_1 \text{ Quotienten } \mu \text{ sind } = 0, \\ \text{die folgenden } \nu_2-\nu_1 \text{ Quotienten } \mu \text{ sind } = 1, \\ \text{die folgenden } \nu_3-\nu_2 \text{ Quotienten } \mu \text{ sind } = 2, \\ \ldots\ldots\ldots\ldots \\ \text{die vorletzten } \nu_{m-1}-\nu_{m-2} \text{ Quotienten } \mu \text{ sind } = m-2, \\ \text{die letzten } \nu_m-\nu_{m-1} \text{ Quotienten } \mu \text{ sind } = m-1. \end{cases}$$

Der Betrag $S\mu$ der *sämmtlichen Quotienten* μ (6.) ist also

35. $$S\mu = 0\nu_1 + 1(\nu_2-\nu_1) + 2(\nu_3-\nu_2) + 3(\nu_4-\nu_3) \ldots \\ \ldots + (m-2)(\nu_{m-1}-\nu_{m-2}) + (m-1)(\nu_m-\nu_{m-1})$$

Daraus folgt, wenn man wegläfst was sich aufhebt,

$S\mu = -\nu_1-\nu_2-\nu_3-\nu_4 \ldots -\nu_{m-1}+(m-1)\nu_m = -S\nu + m\nu_m$ (7.) oder

36. $$S\mu + S\nu = m\nu_m.$$

C. Nun ist in der *letzten* Gleichung (3.) $\nu_m = n$, und in der letzten Gleichung (2.) $\mu_n = m-1$. Denn es kann in $mn = \nu_n m + \varrho_m$ der Rest ϱ_m nur $= 0$ oder $= m$ sein, weil $\nu_m m$ mit m *aufgeht* und also auch ϱ_m mit m aufgehen mufs; eben so kann in $nm = \mu_n n + r_n$ der Rest r_n nur $= 0$ oder $= n$ sein, weil $\mu_n n$ mit n aufgeht und also auch r_n mit n aufgehen mufs. Aber ein $\varrho = m$ *soll* nach (5.) und ein $r = 0$ nach (4.) nicht Statt finden. Also kann in der letzten Gleichung (3.) ϱ_m *nur* $= 0$ und folglich r_m *nur* $= n$ sein, wie es (10.) behauptet, und in der letzten Gleichung (2.) kann r_m *nur* $= n$ und folglich μ_n *nur* $= m-1$ sein, wie es (11.) behauptet.

D. Setzt man dem gemäfs in (36.) für ν_m seinen Werth n, so ergiebt sich

37. $$S\mu + S\nu = mn;$$

welches die Gleichung (12.) des Lehrsatzes ist.

E. Summirt man alle die Gleichungen (2.), so wie diejenigen (3.), so erhält man

38. $$(1+2+3+4 \ldots\ldots + n)m = nS\mu + Sr = \tfrac{1}{2}(n+1)nm \text{ und}$$

39. $$(1+2+3+4 \ldots\ldots + m)n = mS\nu + S\varrho = \tfrac{1}{2}(m+1)mn.$$

In (38.) mit m und in (39.) mit n multiplicirt und die Summe der Producte genommen, giebt

40. $$\tfrac{1}{2}mn(n+1)m + \tfrac{1}{2}mn(m+1)n = mn(S\mu + S\nu) + mSr + nS\varrho,$$

oder, da $S\mu + S\nu = mn$ ist (12.),

$$\tfrac{1}{2}mn[m(n+1)+n(m+1)] = m^2n^2+mSr+nS\varrho \text{ oder}$$

$$41. \quad mSr+nS\varrho = \tfrac{1}{2}mn(m+n);$$

welches die Gleichung (13.) des Lehrsatzes ist.

F. Sind m und n zu einander *theilerfremd*, so sind nach (§. 34.) in (2.) die r die sämmtlichen Zahlen

$$42. \quad 1,\ 2,\ 3,\ 4,\ \ldots\ n-1,\ n.$$

Denn nach (§. 34. I.) würden in (2.) den Factoren 0, 1, 2, 3, ... $n-1$ von m die Reste 0, 1, 2, 3, 4, .. . $n-1$ zukommen, und zu dem Reste 0 gehört der Factor 0 (§. 34. I.). Dieser Factor 0 findet hier nicht Statt, also auch nicht der Rest 0. Dagegen kommt hier der Factor n noch hinzu, und für diesen ist der Rest r zufolge (10.) $=n$. Also sind die r in (2.) nothwendig alle die Zahlen (42.).

Eben so sind die ϱ in (3.) die sämmtlichen Zahlen

$$43. \quad 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ m-1.$$

Denn den Factoren 1, 2, 3, ... $m-1$ in (3.) kommen nach (§. 34. I.) die Reste 1, 2, 3, ... $n-1$ zu, und der zu dem letzten Factor m in (3.) gehörige Rest ϱ_m ist nach (10.) $=0$, so dafs also zusammen die ϱ die Zahlen (43.) sind.

G. Aus (42. und 43.) folgt nun unmittelbar, dafs die Summe der Reste r, nemlich Sr, $=\frac{1}{2}(n+1)n$ und die Summe der Reste ϱ, nemlich $S\varrho$, $=\frac{1}{2}m(m-1)$ ist; wie es (14. u. 15.) behaupten.

H. Setzt man (14. u. 15.) in die Gleichungen (38. u. 39.), welche hier in dem besonderen Fall ebenfalls stattfinden, da sie für *jedes* m und n allgemein gelten; so ergiebt sich

$$44. \quad \tfrac{1}{2}(n+1)mn = nS\mu+\tfrac{1}{2}n(n+1) \text{ und}$$

$$45. \quad \tfrac{1}{2}(m+1)mn = mS\nu+\tfrac{1}{2}m(m-1)$$

oder

$$46. \quad \tfrac{1}{2}m(n+1)-\tfrac{1}{2}(n+1) = S\mu = \tfrac{1}{2}(n+1)(m-1) \text{ und}$$

$$47. \quad \tfrac{1}{2}n(m+1)-\tfrac{1}{2}(m-1) = S\nu = \tfrac{1}{2}((n-1)m+n+1);$$

welches die Gleichungen (16. u. 17.) des Lehrsatzes sind.

J. Aus (16, 17. u. 11.) ergiebt sich

$$48. \quad S\mu-\mu_n = \tfrac{1}{2}(n+1)(m-1)-(m-1) = \tfrac{1}{2}(n-1)(m-1) \text{ und}$$

$$49. \quad S\nu-\nu_m = \tfrac{1}{2}(n-1)m+\tfrac{1}{2}(n+1)-n = \tfrac{1}{2}(n-1)(m-1);$$

wie es der Lehrsatz in (18.) behauptet.

K. Anm. Der Beweis erhält seine Entwicklung besonders durch die Summirung der Gleichungen (34. in *B.*), die ihrerseits aus einfachen Be-

trachtungen hervorgehen. In (*E.*) wird der bekannte Ausdruck der Summe einer sogenannten arithmetischen Reihe zu Hülfe genommen.

§. 38.

Lehrsatz.

Es seien m ***und*** n ***zwei beliebige positive ganze Zahlen und es sei***

$$1.\quad n > m.$$

Man setze

$$2.\ \begin{cases} m = \mu_1 n + r_1, \\ 2m = \mu_2 n + r_2, \\ 3m = \mu_3 n + r_3, \\ \ldots\ldots\ldots\ldots \\ \tfrac{1}{2}(n-1)m = \mu_{\frac{1}{2}(n-1)} n + r_{\frac{1}{2}(n-1)}, \\ \quad \textit{wenn } n \textit{ ungerade und} \\ \tfrac{1}{2}nm = \mu_{\frac{1}{2}n} n + r_{\frac{1}{2}n}, \\ \quad \textit{wenn } n \textit{ gerade ist,} \end{cases} \quad \text{und}\ 3.\ \begin{cases} n = \nu_1 m + \varrho_1, \\ 2n = \nu_2 m + \varrho_2, \\ 3n = \nu_3 m + \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \tfrac{1}{2}(m-1)n = \nu_{\frac{1}{2}(m-1)} m + \varrho_{\frac{1}{2}(m-1)}, \\ \quad \textit{wenn } m \textit{ ungerade und} \\ \tfrac{1}{2}mn = \nu_{\frac{1}{2}m} m + \varrho_{\frac{1}{2}m}, \\ \quad \textit{wenn } m \textit{ gerade ist,} \end{cases}$$

unter der Bedingung, dafs die sämmtlichen r ***und*** ϱ ***positiv sind und dafs***

4. ***die*** r ***aus den Zahlen*** 1, 2, 3, 4, ... n ***und***

5. ***die*** ϱ ***aus den Zahlen*** 0, 1, 2, 3, ... m—1

genommen werden. Ferner bezeichne man die Summe der sämmtlichen Quotienten μ, ***nemlich***

6. $\mu_1 + \mu_2 + \mu_3 \ldots\ldots + \mu_{\frac{1}{2}(n-1)}$ ***oder*** $\mu_{\frac{1}{2}n}$ ***durch*** $S\mu$,

und die Summe der sämmtlichen Quotienten ν, ***nemlich***

7. $\nu_1 + \nu_2 + \nu_3 \ldots\ldots \nu_{\frac{1}{2}(m-1)}$ ***oder*** $\nu_{\frac{1}{2}m}$ ***durch*** $S\nu$.

Alsdann ist

$$8.\ \begin{cases} 1.\ S\mu + S\nu = \tfrac{1}{4}(m-1)(n-1), \\ 2.\ \mu_{\frac{1}{2}(n-1)} = \tfrac{1}{2}(m-1)\ \textit{und}\ r_{\frac{1}{2}(n-1)} = \tfrac{1}{2}(n-m); \end{cases} \ \textit{wenn } m \textit{ ungerade und } n \textit{ ungerade ist;}$$

$$9.\ \begin{cases} 1.\ S\mu + S\nu = \tfrac{1}{4}(m-1)n, \\ 2.\ \mu_{\frac{1}{2}(n-1)} = \tfrac{1}{2}(m-1)\ \textit{und}\ r_{\frac{1}{2}n} = \tfrac{1}{2}n; \end{cases} \ \textit{wenn } m \textit{ ungerade und } n \textit{ gerade ist;}$$

$$10.\ \begin{cases} 1.\ S\mu + S\nu = \tfrac{1}{4}m(n-1), \\ 2.\ \begin{cases} \mu_{\frac{1}{2}(n-1)} = \tfrac{1}{2}m - 1\ \textit{und}\ r_{\frac{1}{2}(n-1)} = n - \tfrac{1}{2}m; \\ \nu_{\frac{1}{2}m} = \tfrac{1}{2}(n-1)\ \textit{und}\ \varrho_{\frac{1}{2}m} = \tfrac{1}{2}m; \end{cases} \end{cases} \ \textit{wenn } m \textit{ gerade und } n \textit{ ungerade ist;}$$

$$11.\ \begin{cases} 1.\ S\mu + S\nu = \tfrac{1}{4}mn, \\ 2.\ \begin{cases} \mu_{\frac{1}{2}n} = \tfrac{1}{2}m - 1\ \textit{und}\ r_{\frac{1}{2}n} = n; \\ \nu_{\frac{1}{2}m} = \tfrac{1}{2}n\ \textit{und}\ \varrho_{\frac{1}{2}m} = 0, \end{cases} \end{cases} \ \textit{wenn } m \textit{ gerade und } n \textit{ gerade ist.}$$

Beispiel 1. für (8.). Es sei

$$12.\quad m = 7,\quad n = 35,$$

so geben (2. u. 3.)

$$13.\ \begin{cases} 1,\ 2,\ 3,\ 4,\ 5m = 0n + 7,\ 14,\ 21,\ 28,\ 35, \\ 6,\ 7,\ 8,\ 9,\ 10m = 1n + 7,\ 14,\ 21,\ 28,\ 35, \\ 11,\ 12,\ 13,\ 14,\ 15m = 2n + 7,\ 14,\ 21,\ 28,\ 35, \\ 16,\ 17m = 3n + 7,\ 14; \end{cases} \text{und } 14.\ \begin{cases} 1.35 = 5.7 + 0, \\ 2.35 = 10.7 + 0, \\ 3.35 = 15.7 + 0; \end{cases}$$

und die Summe sämmtlicher Quotienten ist

$$14.\quad S\mu + S\nu = 5.0 + 5.1 + 5.2 + 2.3 + 5 + 10 + 15 = 51 = \tfrac{1}{4}(7-1)(35-1)$$
$$= \frac{6.34}{4};\ \text{gemäfs } (8.\ 1.).$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 3 = \frac{1}{2}(m-1)$ und $r_{\frac{1}{2}(n-1)} = 14 = \frac{1}{2}(n-m)$; gemäfs (8. 2.).

Beispiel 2. für (8.). Es sei

$$15.\quad m = 9,\quad n = 39,$$

so geben (2. u. 3.)

$$17.\ \begin{cases} 1,\ 2,\ 3,\ 4m = 0n + 9,\ 18,\ 27,\ 36, \\ 5,\ 6,\ 7,\ 8m = 1n + 6,\ 15,\ 24,\ 33, \\ 9,\ 10,\ 11,\ 12,\ 13m = 2n + 3,\ 12,\ 21,\ 30,\ 39, \\ 14,\ 15,\ 16,\ 17m = 3n + 9,\ 18,\ 27,\ 36, \\ 18,\ 19m = 4n + 6,\ 15; \end{cases} \quad 18.\ \begin{cases} 1.39 = 4.9 + 3, \\ 2.39 = 8.9 + 6, \\ 3.39 = 13.9 + 0, \\ 4.39 = 17.9 + 3; \end{cases}$$

also ist die Summe sämmtlicher Quotienten hier

$$19.\quad S\mu + S\nu = 4.0 + 4.1 + 5.2 + 4.3 + 2.4 + 4 + 8 + 13 + 17 = 76$$
$$= \tfrac{1}{4}(9-1)(39-1) = \frac{8.38}{4};\ \text{gemäfs } (8.\ 1.).$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 4 = \frac{1}{2}(m-1)$ und $r_{\frac{1}{2}n} = 15 = \frac{1}{2}(n-m)$; gemäfs (8. 2.).

Beispiel 3. für (9.). Es sei

$$20.\quad m = 21,\quad n = 24,$$

so ist

$$21.\ \left\{\begin{aligned} 1m &= 0n+21,\\ 2m &= 1n+18,\\ 3m &= 2n+15,\\ 4m &= 3n+12,\\ 5m &= 4n+\ 9,\\ 6m &= 5n+\ 6,\\ 7m &= 6n+\ 3,\\ 8m &= 6n+24,\\ 9m &= 7n+21,\\ 10m &= 8n+18,\\ 11m &= 9n+15,\\ 12m &= 10n+12, \end{aligned}\right. \quad \text{und} \quad 22.\ \left\{\begin{aligned} 1n &= 1m+\ 3,\\ 2n &= 2m+\ 6,\\ 3n &= 3m+\ 9,\\ 4n &= 4m+12,\\ 5n &= 5m+15,\\ 6n &= 6m+18,\\ 7n &= 8m+\ 0,\\ 8n &= 9m+\ 3,\\ 9n &= 10m+\ 6,\\ 10n &= 11m+\ 9, \end{aligned}\right.$$

also ist hier

23. $S\mu + S\nu = 61 + 59 = 120 = \frac{1}{4}(21-1)24 = \frac{20.24}{4}$; gemäfs (9. 1.).

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 10 = \frac{1}{2}(m-1)$, $r_{\frac{1}{2}(n-1)} = 12 = \frac{1}{2}n$; gemäfs (9. 2.).

Beispiel 4. für (10.). Es sei

24. $m = 6,\quad n = 15,$

so ist

$$25.\ \left\{\begin{aligned} 1,\ 2m &= 0n+6,\ 12,\\ 3,\ 4,\ 5m &= 1n+3,\ \ 9,\ 15,\\ 6,\ 7m &= 2n+6,\ 12, \end{aligned}\right. \quad \text{und} \quad 26.\ \left\{\begin{aligned} 1n &= 2m+3,\\ 2n &= 5m+0,\\ 3n &= 7m+3, \end{aligned}\right.$$

also ist hier

27. $S\mu + S\nu = 2.0 + 3.1 + 2.2 + 2 + 5 + 7 = 21 = \frac{1}{4}6(15-1) = \frac{6.14}{4}$;

gemäfs (10. 1.). Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 2 = \frac{1}{2}m - 1$, $r_{\frac{1}{2}(n-1)} = 12 = n - \frac{1}{2}m$, $\nu_{\frac{1}{2}m} = 7 = \frac{1}{2}(n-1)$, $\varrho_{\frac{1}{2}m} = 3 = \frac{1}{2}m$; gemäfs (10. 2.).

Beispiel 5. für (11.). Es sei

28. $m = 8,\quad n = 34,$

so ist

$$29.\ \left\{\begin{aligned} 1,\ 2,\ 3,\ 4m &= 0n+8,\ 16,\ 24,\ 32,\\ 5,\ 6,\ 7,\ 8m &= 1n+6,\ 14,\ 22,\ 30,\\ 9,\ 10,\ 11,\ 12m &= 2n+4,\ 12,\ 20,\ 28,\\ 13,\ 14,\ 15,\ 16,\ 17m &= 3n+2,\ 10,\ 18,\ 26,\ 34; \end{aligned}\right. \quad \text{und} \quad 30.\ \left\{\begin{aligned} 1n &= 4m+2,\\ 2n &= 8m+4,\\ 3n &= 12m+6,\\ 4n &= 17m+0, \end{aligned}\right.$$

also ist hier

31. $S\mu + S\nu = 4.0 + 4.1 + 4.2 + 5.3 + 4 + 8 + 12 + 17 = 68 = \frac{1}{4}.8.34$;

gemäfs (11. 1.). Desgleichen ist $\mu_{\frac{1}{2}n} = 3 = \frac{1}{2}m - 1$, $r_{\frac{1}{2}n} = 34 = n$, $\nu_{\frac{1}{2}m} = 17 = \frac{1}{2}n$ und $\varrho_{\frac{1}{2}m} = 0$; gemäfs (11. 2.).

Beweis. ***Erster Fall*** (8.), ***wenn m ungerade und n ungerade ist. A.*** Ganz wie in dem Beweise (§. 37. ***A.***) folgt, dafs die ersten ν_1 Quotienten μ in (2.) Null, die folgenden $\nu_2-\nu_1$ Quotienten $\mu=1$, die folgenden $\nu_3-\nu_2$ Quotienten $\mu=2$ sind, u. s. w.; zuletzt die $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten $=\frac{1}{2}(m-3)$.

B. Nun ist für die ***letzte*** der Gleichungen (2.), nemlich für die Gleichung $\frac{1}{2}(n-1)m=\mu_{\frac{1}{2}(n-1)}n+r_{\frac{1}{2}(n-1)}$,

32. $\frac{1}{2}(n-1)m=\frac{1}{2}mn-\frac{1}{2}m=\frac{1}{2}(m-1)n+\frac{1}{2}(n-m)$.

Hier ist $\frac{1}{2}(n-m)>0$, weil $n>m$ sein soll (1.) und $\frac{1}{2}(n-m)<n$. Auch ist $\frac{1}{2}(n-m)-n=-\frac{1}{2}(n+m)<0$ und $\frac{1}{2}(n-m)+n>n$. Also ist $\frac{1}{2}(n-m)$ der Rest $r_{\frac{1}{2}(n-1)}$, und folglich auch $\frac{1}{2}(m-1)$ aus (32.) der Quotient $\mu_{\frac{1}{2}(n-1)}$, so dafs also

33. $\mu_{\frac{1}{2}(n-1)}=\frac{1}{2}(m-1)$ und $r_{\frac{1}{2}(n-1)}=\frac{1}{2}(n-m)$

ist; wie es (8. 2.) behauptet.

C. Zufolge (***A.***) waren die letzten $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten $\mu=\frac{1}{2}(m-3)$: also auch der $\nu_{\frac{1}{2}(m-1)}$ Quotient μ ist erst $=\frac{1}{2}(m-3)$, und folglich um 1 kleiner als der ***letzte*** $\mu_{\frac{1}{2}(n-1)}$ der überhaupt vorhandenen $\frac{1}{2}(n-1)$ Quotienten, welcher nach (33.) $=\frac{1}{2}(m-1)$ ist. Daraus folgt, dafs zunächst alle die $\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu=0, 1, 2, 3, \ldots \frac{1}{2}(m-3)$ ***vorhanden*** sein müssen, weil kein Quotient μ gröfser ist als der ***letzte*** und sie gruppenweise regelmäfsig um 1 zunehmen: dann aber noch $\frac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu=\frac{1}{2}(m-1)$; denn der ***nächste*** auf den $\nu_{\frac{1}{2}(m-1)}$ten folgende Quotient ist um 1 gröfser als dieser und der ***letzte*** $\mu_{\frac{1}{2}(n-1)}$ ist es nach (33.) ebenfalls.

D. Die Quotienten μ haben also zusammengenommen folgende Werthe:

34.
- die ersten ν_1 Quotienten μ sind $=0$,
- die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$,
- die folgenden $\nu_3-\nu_2$ Quotienten μ sind $=2$,
- die folgenden $\nu_4-\nu_3$ Quotienten μ sind $=3$,
-
- die vorletzten $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten μ sind $=\frac{1}{2}(m-3)$,
- die letzten $\frac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)}$ Quotienten μ sind $=\frac{1}{2}(m-1)$.

Die ***Summe*** der Werthe ***aller*** Quotienten μ ist also

35. $$S\mu=0.\nu_1+1(\nu_2-\nu_1)+2(\nu_3-\nu_2)+3(\nu_4-\nu_3)\ldots$$
$$\ldots+\tfrac{1}{2}(m-3)(\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)})+\tfrac{1}{2}(m-1)(\tfrac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)}),$$

und dieses giebt, wenn man wegläfst was sich aufhebt,

$$S\mu = -\nu_1 - \nu_2 - \nu_3 \ldots\ldots - \nu_{\frac{1}{2}(m-3)} - \nu_{\frac{1}{2}(m-1)} + \tfrac{1}{4}(m-1)(n-1) \quad \text{oder}$$

36. $S\mu + S\nu = \frac{1}{4}(m-1)(n-1)$.

Dieses ist die Gleichung (8. 1.) des Lehrsatzes.

Zweiter Fall (9.), *wenn m ungerade und n gerade ist.*

E. Ganz wie in (*A.*) sind die ersten ν_1 Quotienten μ gleich Null; die folgenden $\nu_2 - \nu_1$ Quotienten $\mu = 1$; die weiter folgenden $\nu_3 - \nu_2$ Quotienten $\mu = 2$ etc., die vorletzten $\nu_{\frac{1}{2}(m-1)} - \nu_{\frac{1}{2}(m-3)}$ Quotienten $\mu = \frac{1}{2}(m-3)$.

F. Sodann aber ist hier für die *letzte* der Gleichungen (2.), nemlich für $\frac{1}{2}nm = \mu_{\frac{1}{2}n} n + r_{\frac{1}{2}n}$,

37. $\frac{1}{2}nm = \frac{1}{2}(m-1)n + \frac{1}{2}n$.

Hier ist $\frac{1}{2}n > 0$ und $< n$. Auch ist $\frac{1}{2}n - n = -\frac{1}{2}n < 0$ und $\frac{1}{2}n + n = \frac{3}{2}n > n$. Also ist $\frac{1}{2}n$ der Rest $r_{\frac{1}{2}n}$ und folglich auch $\frac{1}{2}(m-1)$ in (37.) der Quotient $\mu_{\frac{1}{2}n}$, so dafs also

38. $\mu_{\frac{1}{2}n} = \frac{1}{2}(m-1)$ und $r_{\frac{1}{2}n} = \frac{1}{2}n$

ist, wie es (9. 2.) behauptet.

G. Wiederum wie in (*C.*) folgt, dafs alle die $\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu = 0, 1, 2, 3, \ldots \frac{1}{2}(m-3)$ *vorhanden* sind; und dann noch $\frac{1}{2}n - \nu_{\frac{1}{2}(m-1)}$ um 1 gröfsere Quotienten $\mu = \frac{1}{2}(m-1)$.

H. Die Quotienten μ haben also zusammengenommen folgende Werthe:

39.
- die ersten ν_1 Quotienten μ sind $= 0$,
- die folgenden $\nu_2 - \nu_1$ Quotienten μ sind $= 1$,
- die folgenden $\nu_3 - \nu_2$ Quotienten μ sind $= 2$,
- .
- die vorletzten $\nu_{\frac{1}{2}(m-1)} - \nu_{\frac{1}{2}(m-3)}$ Quotienten μ sind $= \frac{1}{2}(m-3)$,
- die letzten $\frac{1}{2}n - \nu_{\frac{1}{2}(m-1)}$ Quotienten μ sind $= \frac{1}{2}(m-1)$.

Ihre *Summe* beträgt folglich

40. $$S\mu = 0.\nu_1 + 1.(\nu_2 - \nu_1) + 2(\nu_3 - \nu_2) + 3(\nu_4 - \nu_3) \ldots\ldots + \tfrac{1}{2}(m-3)(\nu_{\frac{1}{2}(m-1)} - \nu_{\frac{1}{2}(m-3)}) + \tfrac{1}{2}(m-1)(\tfrac{1}{2}n - \nu_{\frac{1}{2}(m-1)}),$$

und dieses giebt, wenn man wegläfst was sich aufhebt,

$$S\mu = -\nu_2 - \nu_3 - \nu_4 \ldots\ldots - \nu_{\frac{1}{2}(m-3)} - \nu_{\frac{1}{2}(m-1)} + \tfrac{1}{4}(m-1)n \quad \text{oder}$$

41. $S\mu + S\nu = \frac{1}{4}(m-1)n$;

welches die Gleichung (9. 1.) des Lehrsatzes ist.

Dritter Fall (10.), *wenn m gerade und n ungerade ist.*

I. Ganz wie in (*A.*) sind die ersten ν_1 Quotienten μ gleich Null; die folgenden $\nu_2 - \nu_1$ Quotienten μ sind $= 1$, die weiter folgenden $\nu_3 - \nu_2$ Quotienten

$\mu = 2$ etc. Die letzte Gleichung (3.) ist aber hier $\frac{1}{2}mn = \nu_{\frac{1}{2}m}m + \varrho_{\frac{1}{2}m}$, also steigt ν bis $\nu_{\frac{1}{2}m}$, und folglich sind die letzten Quotienten μ diejenigen $\nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}m-1}$, und ihr Werth ist $= \frac{1}{2}m - 1$.

K. Sodann ist für die letzte der Gleichungen (2.), nemlich für $\frac{1}{2}(n-1)m = \mu_{\frac{1}{2}(n-1)}n + r_{\frac{1}{2}(n-1)}$,

42. $$\frac{1}{2}(n-1)m = (\frac{1}{2}m-1)n + n - \frac{1}{2}m.$$

Hier ist $n - \frac{1}{2}m > 0$, weil $n > m$ sein soll, und zugleich $n - \frac{1}{2}m < n$. Auch ist $n - \frac{1}{2}m - n = -\frac{1}{2}m < 0$ und $n - \frac{1}{2}m + n = 2n - \frac{1}{2}m > n$. Also ist $n - \frac{1}{2}m$ der Rest $r_{\frac{1}{2}(n-1)}$, und folglich auch, aus (42.), $\frac{1}{2}m - 1$ der Quotient $\mu_{\frac{1}{2}(n-1)}$, so dafs

43. $$\mu_{\frac{1}{2}(n-1)} = \frac{1}{2}m - 1 \quad \text{und} \quad r_{\frac{1}{2}(n-1)} = n - \frac{1}{2}m$$

ist, wie es (10. 2.) behauptet.

L. Hieraus folgt, dafs es aufser den letzten $\nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}(m-1)}$ Quotienten μ in (*I.*), deren Werth schon $\frac{1}{2}m - 1$ war, ***keine*** weiter giebt. Denn der Werth des ***letzten*** $\frac{1}{2}(n-1)$ten μ in (2.) ist nach (43.) auch nur $= \frac{1}{2}m - 1$. So folgt denn also auch, dafs hier $\nu_{\frac{1}{2}m}$ selbst $= \frac{1}{2}(n-1)$ sein mufs. In der That ist für die letzte Gleichung $\frac{1}{2}mn = \nu_{\frac{1}{2}m}m + \varrho_{\frac{1}{2}m}$ in (3.)

44. $$\frac{1}{2}mn = \frac{1}{2}(n-1)m + \frac{1}{2}m.$$

Hier ist $\frac{1}{2}m > 0$ und $< m$, also ist $\frac{1}{2}m$ der Rest $\varrho_{\frac{1}{2}m}$ und folglich auch $\frac{1}{2}(n-1)$ der Quotient $\nu_{\frac{1}{2}m}$, so dafs also

45. $$\nu_{\frac{1}{2}m} = \frac{1}{2}(n-1) \quad \text{und} \quad \varrho_{\frac{1}{2}m} = \frac{1}{2}m$$

ist, wie es (10. 2.) behauptet.

M. Es sind also in dem gegenwärtigen dritten Falle überhaupt nur die in (*I.*) verzeichneten Quotienten μ vorhanden, und $\nu_{\frac{1}{2}m}$ ist $= \frac{1}{2}(n-1)$. Die Quotienten haben also folgende Werthe:

46. $$\begin{cases} \text{die ersten } \nu_1 \text{ Quotienten } \mu \text{ sind } = 0, \\ \text{die folgenden } \nu_2 - \nu_1 \text{ Quotienten } \mu \text{ sind } = 1, \\ \text{die folgenden } \nu_3 - \nu_2 \text{ Quotienten } \mu \text{ sind } = 2, \\ \text{die folgenden } \nu_4 - \nu_3 \text{ Quotienten } \mu \text{ sind } = 3, \\ \dots\dots\dots\dots\dots\dots \\ \text{die \textit{letzten} } \nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}m-1} \text{ \textit{oder} } \frac{1}{2}(n-1) - \nu_{\frac{1}{2}m-1} \text{ Quotienten } \mu \text{ sind } = \frac{1}{2}m - 1. \end{cases}$$

Ihre Summe beträgt demnach

47. $$S\mu = 0\nu_1 + 1(\nu_2 - \nu_1) + 2(\nu_3 - \nu_2) \dots + (\tfrac{1}{2}m-2)(\nu_{\frac{1}{2}m-1} - \nu_{\frac{1}{2}m-2}) + (\tfrac{1}{2}m-1)(\tfrac{1}{2}(n-1) - \nu_{\frac{1}{2}m-1}),$$

oder, wenn man wegläfst was sich aufhebt,

48. $$S\mu = -\nu_1 - \nu_2 - \nu_3 \dots \nu_{\frac{1}{2}m-2} - \nu_{\frac{1}{2}m-1} + (\tfrac{1}{2}m-1).\tfrac{1}{2}(n-1).$$

Dieses ist, da $\nu_1+\nu_2+\nu_3 \ldots\ldots+\nu_{\frac{1}{2}m-1} = S\nu-\nu_{\frac{1}{2}m}$ (7.) $= S\nu-\frac{1}{2}(n-1)$ (45.) ist, so viel als

$$S\mu = -S\nu+\frac{1}{2}(n-1)+(\frac{1}{2}m-1)\frac{1}{2}(n-1) \text{ oder}$$

49. $$S\mu+S\nu = \frac{1}{4}m(n-1);$$

und dieses ist die Gleichung (10. 1.) des Lehrsatzes.

Vierter Fall (11), *wenn m gerade und n gerade ist.* ***N.*** Ganz wie in (*A.*) sind die ersten ν Quotienten $\mu=0$, die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$; die folgenden $\nu_3-\nu_2$ Quotienten μ sind $=2$, u. s. w. Die letzte Gleichung (3.) ist hier $\frac{1}{2}mn=\nu_{\frac{1}{2}m}m+\varrho_{\frac{1}{2}m}$, also steigt hier ν bis $\nu_{\frac{1}{2}m}$; die letzten Quotienten μ sind hier diejenigen $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ und ihr Werth ist $=\frac{1}{2}m-1$.

O. Diese Quotienten μ kommen auch wirklich alle vor, und keiner mehr: denn die letzte der Gleichungen (2.) ist hier $\frac{1}{2}nm=\mu_{\frac{1}{2}n}n+r_{\frac{1}{2}n}$. Aus derselben folgt, dafs $r_{\frac{1}{2}n}$ mit n *aufgehen* und folglich $=n$ sein mufs, da die r nicht 0 und nicht $>n$ sein sollen (4.). Mithin ist hier nothwendig

50. $$\mu_{\frac{1}{2}n} = \frac{1}{2}m-1 \quad\text{und}\quad r_{\frac{1}{2}n} = n;$$

wie es (11. 2.) behauptet. Ähnlich folgt aus der letzten Gleichung (3.), welche $\frac{1}{2}mn=\nu_{\frac{1}{2}m}m+\varrho_{\frac{1}{2}m}$ ist, dafs $\varrho_{\frac{1}{2}m}$ mit m *aufgehen* und also $=0$ sein mufs, da die ϱ nicht gröfser als $m-1$ sein sollen (5.), so dafs also

51. $$\nu_{\frac{1}{2}m} = \frac{1}{2}n \quad\text{und}\quad \varrho_{\frac{1}{2}m} = 0$$

sein mufs; gemäfs (11. 2.). Die $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ Quotienten in (*N.*), an Werth $\frac{1}{2}m-1$, sind also die *letzten* μ, denn es sind nur $\frac{1}{2}n$ Quotienten μ in (2.) vorhanden, und $\nu_{\frac{1}{2}m}$ ist $=\frac{1}{2}n$ (51.); desgleichen ist der Werth *des* letzten $\mu_{\frac{1}{2}n}$ oder *der* letzten $\mu=\frac{1}{2}m-1$ (50.); wie es für die $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ letzten Quotienten sein soll.

P. Die Quotienten μ haben also in dem gegenwärtigen vierten Falle folgende Werthe:

52.
$$\begin{cases} \text{die ersten } \nu_1 \text{ Quotienten } \mu \text{ sind } = 0, \\ \text{die folgenden } \nu_2-\nu_1 \text{ Quotienten } \mu \text{ sind } = 1, \\ \text{die folgenden } \nu_3-\nu_2 \text{ Quotienten } \mu \text{ sind } = 2, \\ \text{die folgenden } \nu_4-\nu_3 \text{ Quotienten } \mu \text{ sind } = 3, \\ \ldots\ldots\ldots\ldots \\ \text{die \textit{letzten} } \nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1} \text{ \textit{oder} } \frac{1}{2}n-\nu_{\frac{1}{2}m-1} \text{ Quotienten } \mu \text{ sind } = \frac{1}{2}m-1. \end{cases}$$

Ihre *Summe* beträgt daher

53. $$S\mu = 0.\nu_1+1(\nu_2-\nu_1)+2(\nu_3-\nu_2)\ldots\ldots+(\frac{1}{2}m-2)(\nu_{\frac{1}{2}m-1}-\nu_{\frac{1}{2}m-2}) \\ +(\frac{1}{2}m-1)(\frac{1}{2}n-\nu_{\frac{1}{2}m-1}),$$

oder, wenn man wegläfst was sich aufhebt,

54. $S\mu = -\nu_1 - \nu_2 - \nu_3 \ldots\ldots -\nu_{\frac{1}{2}m-2} - \nu_{\frac{1}{2}m-1} + (\frac{1}{2}m-1)\frac{1}{2}n.$

Dieses ist, da $\nu_1 + \nu_2 + \nu_3 \ldots\ldots + \nu_{\frac{1}{2}m-1} = S\nu - \nu_{\frac{1}{2}m}$ (7.) $= S\nu - \frac{1}{2}n$ (51.) ist, so viel als

$$S\mu = -S\nu + \frac{1}{2}n + (\frac{1}{2}m-1)\frac{1}{2}n \text{ oder}$$

55. $S\mu + S\nu = \frac{1}{4}mn;$

und dieses ist die Gleichung (11. 1.) des Lehrsatzes.

Q. Anm. Der Beweis ist im Wesentlichen dem des einfacheren Falles im vorigen Paragraph nachgebildet. Es ist wieder die Summirung der Gleichungen (34. 39. 46. und 52.), durch welche er insbesondere seine Entwickelung erhält. Eigenthümlich sind übrigens die aus willkürlicher Zertheilung eines Ausdrucks wie (32. 37. u. 42.) hergenommenen Folgerungen.

§. 39.

Lehrsatz.

Es sei u *eine beliebige ungerade positive ganze Zahl, die also nach* (§. 28. 10.) *immer durch*

1. $u = 4n \pm 1$

ausgedrückt werden kann, wo n *eine positive ganze Zahl bezeichnet. Eine andere, zu* u *theilerfremde beliebige positive ganze Zahl sei* v. *Man setze*

2. $$\begin{cases} v = \mu_1 u + r_1, \\ 2v = \mu_2 u + r_2, \\ 3v = \mu_3 u + r_3, \\ 4v = \mu_4 u + r_4, \\ \ldots\ldots\ldots\ldots\ldots \\ \frac{1}{2}(u-1)v = \mu_{\frac{1}{2}(u-1)} u + r_{\frac{1}{2}(u-1)}; \end{cases}$$

unter der Bedingung, dafs die sämmtlichen $r > 0$ *und* $< u$ *sind, und bezeichne*

3. *die Anzahl der Reste* r *in* (2.), *welche* $> \frac{1}{2}u$ *sind, durch* $\varkappa$ *und die Summe der sämmtlichen Quotienten* μ *in* (2.), *also*

4. $\mu_1 + \mu_2 + \mu_3 + \mu_4 \ldots\ldots + \mu_{\frac{1}{2}(u-1)}$ *durch* $S\mu$.

Alsdann ist

5. $\varkappa$ *gerade oder ungerade, je nachdem es die Zahl* $s = n(v-1) + S\mu$ *ist.*

Ist auch v *ungerade, eben wie* u, *so ist*

6. $\varkappa$ *gerade oder ungerade, je nachdem es* $S\mu$ *ist.*

Beispiel 1. Es sei

7. $u = 4n - 1 = 11$, also $n = 3$, $\frac{1}{2}(u-1) = 5$, $v = 15$.

Alsdann giebt (2.)

$$8. \quad \begin{cases} v = 1u + 4, \\ 2v = 2u + 8, \\ 3v = 3u + 12, \\ 4v = 5u + 5, \\ 5v = 6u + 9; \end{cases}$$

also ist in (5.)

$$9. \quad s = 3.14 + 1 + 2 + 3 + 5 + 6 = 59.$$

Die 3 Reste 8, 12 und 9 sind $> \frac{1}{2}u (= 5\frac{1}{2})$, also ist

$$10. \quad \varkappa = 3,$$

und s und $\varkappa$ sind, gemäfs (5.), beide ***zugleich ungerade.***

Desgleichen sind gemäfs (6.) hier, wo auch v ***ungerade*** ist, $\varkappa = 3$ und $S\mu = 1 + 2 + 3 + 5 + 6 = 17$ ***beide zugleich ungerade.***

Beispiel 2. Es sei

11. $u = 4n + 1 = 13$, also $n = 3$, $\frac{1}{2}(u-1) = 6$; $v = 18$.

Alsdann giebt (2.)

$$12. \quad \begin{cases} v = 1u + 5, \\ 2v = 2u + 10, \\ 3v = 3u + 15, \\ 4v = 5u + 7, \\ 5v = 6u + 12, \\ 6v = 8u + 4; \end{cases}$$

also ist in (5.)

$$13. \quad s = 3.17 + 1 + 2 + 3 + 5 + 6 + 8 = 76.$$

Die 4 Reste 10, 15, 7 und 12 sind $> \frac{1}{2}u \ (= 6\frac{1}{2})$, also ist

$$14. \quad \varkappa = 4;$$

und s und $\varkappa$ sind, gemäfs (5.), beide ***zugleich gerade***

Beweis ***A.*** Es sei für ein beliebiges εfache von v:

$$15. \quad \varepsilon v = \mu_\varepsilon u + r_\varepsilon,$$

welche Gleichung, wenn man darin $\varepsilon = 1, 2, 3, \ldots \frac{1}{2}(u-1)$ setzt, die Gleichungen (2.) giebt. Die Gleichung (15.), mit 2 multiplicirt, giebt

$$16. \quad 2\varepsilon v = 2\mu_\varepsilon u + 2r_\varepsilon.$$

Setzt man nun in (16.) der Reihe nach $\varepsilon = 1, 2, 3, \ldots \frac{1}{2}(u-1)$ und in (15.) der Reihe nach $\varepsilon = 2, 4, 6, 8, \ldots u-1$, so erhält man folgende ***zwiefachen*** Ausdrücke von $2v$, $4v$, $6v$, ... $(u-1)v$, nemlich:

$$17.\quad \begin{cases} 2v = 2\mu_1 u + 2r_1 = \mu_2 u + r_2, \\ 4v = 2\mu_2 u + 2r_2 = \mu_4 u + r_4, \\ 6v = 2\mu_3 u + 2r_3 = \mu_6 u + r_6, \\ 8v = 2\mu_4 u + 2r_4 = \mu_8 u + r_8, \\ \dots\dots\dots\dots\dots \\ (u-1)v = 2\mu_{\frac{1}{2}(u-1)} u + 2r_{\frac{1}{2}(u-1)} = \mu_{u-1} u + r_{u-1}. \end{cases}$$

In den ersten dieser Ausdrücke von $2v, 4v, 6v, \dots (v-1)$ kommen alle die Reste $r_1, r_2, r_3, \dots r_{\frac{1}{2}(u-1)}$ vor, die sich in (2.) finden, und der *allgemeine* Ausdruck der Gleichungen (17.) ist

$$18.\quad 2\varepsilon v = 2\mu_\varepsilon u + 2r_\varepsilon = \mu_{2\varepsilon} u + r_{2\varepsilon};$$

wo $\varepsilon = 1, 2, 3, \dots \frac{1}{2}(u-1)$ sein kann.

B. *a.* Ist in (18.) $r_\varepsilon < \frac{1}{2}u$, so ist $2r_\varepsilon < u$ und zugleich > 0. ***Eben das*** ist $r_{2\varepsilon}$, und es giebt nur einen positiven Rest > 0 und $< u$ für ein bestimmtes ε; also ist nothwendig $r_{2\varepsilon} = 2r_\varepsilon$, und folglich auch

$$19.\quad 2\mu_\varepsilon = \mu_{2\varepsilon},\ \textit{wenn}\ r_\varepsilon < \tfrac{1}{2}u.$$

b. Ist hingegen in (18.) $r_\varepsilon > \frac{1}{2}u$, so ist $2r_\varepsilon > u$; also müfste der Quotient $2\mu_\varepsilon$ um 1 ***gröfser*** genommen werden, wenn $2r_\varepsilon = r_{2\varepsilon}$ sein sollte. Mithin ist nothwendig

$$20.\quad 2\mu_\varepsilon = \mu_{2\varepsilon} - 1,\ \textit{wenn}\ r_\varepsilon > \tfrac{1}{2}u.$$

c. ***Gleich*** $\frac{1}{2}u$ kann r nicht sein, weil nach der Voraussetzung u ***ungerade*** sein soll. Es kommen also in (17.) ***nur*** Reste $r < \frac{1}{2}u$ oder $r > \frac{1}{2}u$ vor.

C. Nun kommen in (17.), wie schon bemerkt, ***alle*** die Reste $r_1, r_2, r_3, \dots r_{\frac{1}{2}(u-1)}$ vor, und $\varkappa$ derselben sind nach der Voraussetzung $> \frac{1}{2}u$: also ist in jeder von $\varkappa$ ***Gleichungen*** (17.) nach (***B. b.***) der Quotient μ ***links*** um ***1 gröfser*** als der Quotient μ ***rechts;*** in den ***übrigen*** $\frac{1}{2}(u-1) - \varkappa$ Gleichungen dagegen sind nach (***B. a.***) die Quotienten μ links und rechts einander ***gleich.***

Nimmt man also links und rechts die ***Summe*** aller Quotienten μ, so ergiebt sich

$$21.\quad 2\mu_1 + 2\mu_2 + 2\mu_3 \dots + 2\mu_{\frac{1}{2}(u-1)} = \mu_2 + \mu_4 + \mu_6 \dots \mu_{u-1} - \varkappa,$$

oder, wenn man

$$22.\quad \mu_2 + \mu_4 + \mu_6 \dots + \mu_{u-1}\ \text{durch}\ S_2\mu$$

bezeichnet,

$$23.\quad \varkappa = S_2\mu - 2S\mu\ (4.).$$

Aber $2S\mu$ ist *immer* eine *gerade* Zahl: also ist $\varkappa$ *gerade* oder ungerade, je nachdem es $S_2\mu$ (22.) ist.

D. Man setze in (15.) $u-\varepsilon$ statt ε, so ergiebt sich

$$24.\quad (u-\varepsilon)v = \mu_{u-\varepsilon}u + r_{u-\varepsilon},$$

und wenn man (15.) zu (24.) addirt,

$$25.\quad \varepsilon v + (u-\varepsilon)v \text{ oder } uv = (\mu_\varepsilon + \mu_{u-\varepsilon})u + r_\varepsilon + r_{u-\varepsilon}.$$

Daraus folgt, dafs $r_\varepsilon + r_{u-\varepsilon}$ mit u *aufgehen* mufs (§. 18.). Es sind aber r_ε und $r_{u-\varepsilon}$ beide >0 und $<u$, also ist $r_\varepsilon + r_{u-\varepsilon} > 0$ und $<2u$. Daher mufs nothwendig

$$26.\quad r_\varepsilon + r_{u-\varepsilon} = u$$

sein. Mithin ist in (25.)

$$27.\quad uv = (\mu_\varepsilon + \mu_{u-\varepsilon})u + u,$$

und folglich, mit u dividirt, $v = \mu_\varepsilon + \mu_{u-\varepsilon} + 1$ oder

$$28.\quad \mu_{u-\varepsilon} = v - 1 - \mu_\varepsilon.$$

E. Man setze nun in (28.) der Reihe nach $\varepsilon = 1, 3, 5, 7 \ldots\ldots 2n-1$, so ergiebt sich

$$29.\quad \begin{cases} \mu_{u-1} = v-1-\mu_1, \\ \mu_{u-3} = v-1-\mu_3, \\ \mu_{u-5} = v-1-\mu_5, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mu_{u-2n+1} = v-1-\mu_{2n-1}. \end{cases}$$

Die *Anzahl* dieser Gleichungen ist n; denn wäre nur 1 Gleichung vorhanden, so würde der Zeiger 1 von μ rechterhand durch $2.1-1=1$ ausgedrückt werden; wären 2 Gleichungen vorhanden, der Zeiger 3 von μ durch $2.2-1=3$; wären 3 Gleichungen vorhanden, der Zeiger 5 von μ durch $2.3-1=5$, u. s. w.: allgemein, wenn n Gleichungen vorhanden wären, der Zeiger von μ durch $2.n-1$; und das ist wirklich der Zeiger von μ. Die *Summe* der Gleichungen (29.) ist also

$$30.\quad \mu_{u-1} + \mu_{u-3} + \mu_{u-5} \ldots\ldots + \mu_{u-2n+1} = n(v-1) - (\mu_1 + \mu_3 + \mu_5 \ldots\ldots + \mu_{2n-1}).$$

F. Der Ausdruck (22.) ist so viel als

$$31.\quad \left.\begin{aligned} S_2\mu = \mu_2 + \mu_4 + \mu_6 \ldots\ldots + \mu_{2n} \\ + \mu_{u-1} + \mu_{u-3} + \mu_{u-5} \ldots\ldots \mu_{u-2n+1} \end{aligned}\right\} \text{ für } u = 4n+1 \text{ und}$$

$$32.\quad \left.\begin{aligned} S_2\mu = \mu_2 + \mu_4 + \mu_6 \ldots\ldots + \mu_{2n-2} \\ + \mu_{u-1} + \mu_{u-3} + \mu_{u-5} \ldots\ldots + _{u-2n+1} \end{aligned}\right\} \text{ für } u = 4n-1;$$

denn

33. $\begin{cases} \text{für } u = 4n+1 \text{ ist } u - 2n + 1 = 2n + 2, \text{ also } \textit{folgt } \mu_{u-2n+1} = u_{2n+1} \\ \qquad \text{in (31.) unmittelbar } \textit{auf } u_{2n}, \text{ und} \\ \text{für } u = 4n+1 \text{ ist } u - 2n + 1 = 2n, \text{ also } \textit{folgt } \mu_{u-2n+1} = u_{2n} \\ \qquad \text{in (32.) unmittelbar } \textit{auf } u_{2n-2}. \end{cases}$

Setzt man nun in (31. u. 32.) für die *untere* Zeile ihre Werthe aus (30.), so ergiebt sich

34. $$S_2\mu = \mu_2 + \mu_4 + \mu_6 \dots + \mu_{2n} + n(v-1) - (\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1})$$
für $u = 4n+1$ und

35. $$S_2\mu = \mu_2 + \mu_4 + \mu_6 \dots + \mu_{2n-2} + n(v-1) - (\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1})$$
für $u = 4n-1$.

G. Addirt man in (34. u. 35.) auf beiden Seiten noch
$$2(\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1}),$$
so ergiebt sich

36. $$\begin{aligned} S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1}) &= \mu_2 + \mu_4 + \mu_6 \dots + \mu_{2n} + n(v-1) \\ &\quad + \mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1} \\ &= \mu_1 + \mu_2 + \mu_3 + \mu_4 \dots + \mu_{2n} + n(v-1) \end{aligned}$$
für $u = 4n+1$ und

37. $$\begin{aligned} S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1}) &= \mu_2 + \mu_4 + \mu_6 \dots + \mu_{2n-2} + n(v-1) \\ &\quad + \mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-3} + \mu_{2n-1} \\ &= \mu_1 + \mu_2 + \mu_3 + \mu_4 \dots + \mu_{2n-1} + n(v-1) \end{aligned}$$
für $u = 4n-1$.

Es ist aber in (36.) das letzte μ_{2n} rechts $= \mu_{\frac{1}{2}(u-1)}$, da $2n = \frac{1}{2}(u-1)$ ist für $u = 4n+1$, und in (37.) ist das letzte u_{2n-1} rechts *ebenfalls* $= \mu_{\frac{1}{2}(u-1)}$, da $2n-1 = \frac{1}{2}(u-1)$ ist für $u = 4n-1$. Also geben (36. u. 37.) gleichmäfsig ***Dasselbe,*** nemlich
$$S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1}) = \mu_1 + \mu_2 + \mu_3 + \mu_4 \dots + \mu_{\frac{1}{2}(u-1)} + n(v-1)$$
oder

38. $$S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 \dots + u_{2n-1}) = S\mu + n(v-1) \text{ (4.)}.$$

Die hier zu $S_2\mu$ links addirte Zahl $2(\mu_1 + \mu_3 + \mu_5 \dots + \mu_{2n-1})$, welche sie auch sein mag, ist aber ***immer gerade:*** also ist $S_2\mu$ ***gerade*** oder ***ungerade,*** je nachdem es $S\mu + n(v-1)$ ist. Nun war $\varkappa$ ***gerade*** oder ***ungerade,*** je nachdem es $S_2\mu$ ist (*C.*): also ist $\varkappa$ ***gerade*** oder ***ungerade,*** je nachdem es $S\mu + n(v-1)$ ist.

Dieses ist was der Lehrsatz in (5.) behauptet.

H. Ist auch v ***ungerade***, gleichwie u, so ist $v-1$ ***gerade,*** also auch $n(v-1)$ ***gerade.*** Also ist $\varkappa$ ***gerade*** oder ***ungerade,*** je nachdem es blofs $S\mu$ ist; gemäfs (6.).

1. Anm. Der Beweis des Satzes entwickelt sich insbesondere aus den *zwiefachen* Ausdrücken (17.) der *geraden* Vielfachen $2v$, $4v$, $6v$, ... von v.

§. 40.

Lehrsatz.

Wenn p ***eine beliebige Stammzahl ist, so bleibt, wenn man die*** p—1te ***Potenz jeder beliebigen positiven oder negativen Zahl*** z, ***die nicht mit*** p ***aufgeht, durch*** p ***dividirt, immer der Rest*** +1: ***das heifst, die Gleichung***

$$1.\quad z^{p-1} = \mathfrak{G}p + 1$$

findet für jede Stammzahl p ***und für jeden beliebigen positiven oder negativen Werth von*** z ***Statt, der nicht mit*** p ***aufgeht. Jedoch findet sie nicht nothwendig Statt, wenn*** p ***nicht eine Stammzahl ist, sondern Factoren*** >1 ***hat.***

Diesen Satz nennt man gewöhnlich, nach seinem Erfinder, den Fermatschen Satz.

Auch ist immer

$$2.\quad z^{p-1} = \mathfrak{G}(z^{\delta}-1)p + 1,$$

wo δ ***einen beliebigen Theiler von*** p—1 ***bezeichnet.***

Beispiele. 1. Es sei

$$3.\quad p = 13.$$

Ist hier z. B. $z = 11$, so ist $z^2 = 121 = \mathfrak{G}13 + 4$, $z^4 = \mathfrak{G}13 + 16 = \mathfrak{G}13 + 3$, $z^8 = \mathfrak{G}.13 + 9$, $z^{12} = z^{p-1} = z^4.z^8 = (\mathfrak{G}13+3)(\mathfrak{G}13+9) = \mathfrak{G}13 + 27 = \mathfrak{G}13 + 1$; gemäfs (1.).

Ist $z = 2$, so ist $z^3 = 8$, $z^6 = 64 = \mathfrak{G}p - 1$, $z^{12} = z^{p-1} = \mathfrak{G}p + 1$; ebenfalls gemäfs (1.); und so giebt *jedes* andere, nicht durch p theilbare z, $z^{p-1} = \mathfrak{G}p + 1$. Ist $z > p$, so ist es so viel als $z = \mathfrak{G}p + z_1$, wo nun $z_1 < p$. Ist z *negativ*, so hat z^{p-1} gleichwohl denselben Rest $+1$, indem der Exponent $p-1$ von z für $p = 13$ und für jede andere *ungerade* Stammzahl *gerade* ist.

2. Es sei

$$4.\quad p = 2,$$

so ist $p - 1 = 1$ und also $z^{p-1} = z$ selbst. Alle mit $p = 2$ nicht aufgehenden Zahlen, das heifst alle *ungeraden* positiven und negativen Zahlen lassen aber, durch 2 dividirt, offenbar den Rest $+1$. Z. B.: -15 ist gleich $-8.2 + 1$. Also auch für die einzige *gerade* Stammzahl $p = 2$ findet der Satz Statt.

Beweis *A.* Es kann immer

$$5.\quad mz = \mathfrak{G}p + r,$$

gesetzt werden, wo, wenn m eine *beliebige* ganze Zahl bedeutet,

$$6.\quad r \text{ eine der Zahlen } 1, 2, 3, 4, \ldots p-1$$

ist, aber nicht 0 sein kann, weil z nicht mit p aufgehen soll.

B. Giebt man nun dem beliebigen m der Reihe nach die Werthe $1, 2, 3, 4, \ldots p-1$, so durchläuft nach (§. 34. I.) auch r alle die Werthe $1, 2, 3, 4, \ldots p-1$, obwohl in verschiedener Ordnung. Es ergeben sich also die $p-1$ Gleichungen

$$7.\quad \begin{cases} 1z = \mathfrak{G}p + r_1, \\ 2z = \mathfrak{G}p + r_2, \\ 3z = \mathfrak{G}p + r_3, \\ \ldots\ldots\ldots\ldots \\ (p-1)z = \mathfrak{G}p + r_{p-1}; \end{cases}$$

wo die r nun nothwendig alle die Zahlen $1, 2, 3, 4 \ldots p-1$ sind.

C. Multiplicirt man diese $p-1$ Gleichungen in einander, so ergiebt sich

$$8.\quad 1.2.3.4\ldots(p-1).z^{p-1} = \mathfrak{G}p + r_1 r_2 r_3 r_4 \ldots r_{p-1},$$

und hieraus

$$9.\quad 1.2.3.4\ldots(p-1).z^{p-1} = \mathfrak{G}p + 1.2.3.4\ldots(p-1).$$

D. Aus (9.) folgt

$$10.\quad 1.2.3.4\ldots(p-1)(z^{p-1}-1) = \mathfrak{G}p.$$

Hier geht die Stammzahl p in *keinen* der Factoren $1, 2, 3, 4, \ldots p-1$ auf; denn alle sind $< p$. Also geht p auch in dem Producte $1.2.3.4\ldots p-1$ nicht auf (§. 22.). Da nun aber nach (8.) p nothwendig in die gesammte Gröfse $1.2.3.4\ldots(p-1)(z^{p-1}-1)$ aufgehen *mufs*, so mufs es in den noch übrigen Factor $z^{p-1}-1$ aufgehen (§. 25.) und also

$$11.\quad z^{p-1}-1 = \mathfrak{G}p$$

sein; woraus die Gleichung (1.) des Lehrsatzes folgt.

E. Alles Vorige bleibt dasselbe, wie grofs oder klein auch die Zahl z sein und ob sie positiv oder negativ sein mag, wenn sie nur nicht mit p aufgeht. Aber in diesem, und nur in diesem einzigen Falle von z findet das Bewiesene *nicht* Statt, indem dann r nicht eine der Zahlen (5.), sondern für *jedes* m gleich *Null* ist Mithin gilt die Gleichung (1.) für jeden beliebigen positiven oder negativen ganzzahligen Werth von z, der *nicht* mit p aufgeht.

F. Ist p *nicht* eine *Stammzahl,* so findet zwar noch für jedes zu p *theilerfremde* z zufolge (§. 34.) Alles Statt, was oben (*A.*, *B.*, *C.*) behaupten,

denn auch dann noch sind die r nothwendig alle die Zahlen $1, 2, 3, 4, \ldots p-1$ (§. 34. I.), aber aus der Gleichung (10.) folgt nun nicht mehr, dafs nothwendig $z^{p-1}-1$ mit p aufgehen mufs, weil schon einzelne Factoren von p in $1, 2, 3, 4 \ldots p-1$ aufgehen können.

G. Nach (1.) ist $z^{p-1}-1 = \mathfrak{S}p$. Aber $z^{p-1}-1$ geht für *jedes* z und $p-1$ mit $z^\delta-1$ auf, wenn δ in $p-1$ aufgeht, und giebt $z^{p-1-\delta}+z^{p-1-2\delta}+z^{p-1-3\delta}\ldots+1$ zum Quotienten. Also mufs auch $\mathfrak{S}p$ mit $z^\delta-1$ aufgehen. Aber die Stammzahl p geht *nicht* mit $z^\delta-1$ auf, also mufs $\mathfrak{S}$ mit $z^\delta-1$ aufgehen und folglich

$$12.\quad z^{p-1}-1 = \mathfrak{S}(z^\delta-1)p$$

sein; woraus die Gleichung (2.) folgt.

Anm. *H.* Der Beweis beruht insbesondere auf dem Umstande, dafs in (7.) die r nach (§. 34.) nothwendig alle die Zahlen $1, 2, 3, \ldots p-1$ selbst sind.

Der *Fermat*sche Lehrsatz findet in der gesammten Theorie der Zahlen vielfache Anwendungen und ist also als einer der Hauptsätze derselben zu betrachten. Wie er sich ändert, wenn p *nicht* eine Stammzahl ist, wird weiter unten vorkommen

§. 41.

Lehrsatz.

Es sei p *eine beliebige Stammzahl* >2, z *eine beliebige ganze Zahl, die nicht mit* p *aufgeht.*

Man setze

$$1.\quad \left\{\begin{aligned} z &= \mathfrak{S}p+r_1,\\ 2z &= \mathfrak{S}p+r_2,\\ 3z &= \mathfrak{S}p+r_3,\\ 4z &= \mathfrak{S}p+r_4,\\ &\ldots\\ \tfrac{1}{2}(p-1)z &= \mathfrak{S}p+r_{\frac{1}{2}(p-1)},\end{aligned}\right.$$

und bezeichne

2. *die Anzahl der Reste* r *in* (1.), *welche* $>\frac{1}{2}$p *sind, durch* z.

Alsdann ist

$$3.\quad z^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1,\ \textit{wenn } z \textit{ gerade, und}$$

$$4.\quad z^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1,\ \textit{wenn } z \textit{ ungerade ist.}$$

Das Eine und das Andere findet jedoch nothwendig nur dann Statt, wenn p *eine Stammzahl ist; nicht nothwendig, wenn* p *Theiler* >1 *hat.*

Beispiel 1. Es sei

5. $p = 13, \quad z = 20,$

so giebt (1.)

6. $1, 2, 3, 4, 5, 6 . z = \mathfrak{S}p + 7, 1, 8, 2, 9$ und $3.$

Die 3 Reste 7, 8 und 9 sind $> \frac{1}{2}p$, also ist $\varkappa = 3$ und *ungerade*. $z^{\frac{1}{2}(p-1)}$ ist $20^6 = \mathfrak{S}p + 7^6 = \mathfrak{S}p + 49^3 = \mathfrak{S}p - 3^3 = \mathfrak{S}p - 27 = \mathfrak{S}p - 1$; wie es nach (4.) sein soll.

Beispiel 2. Es sei

7. $p = 19, \quad z = 42,$

so giebt (1.)

8. $1, 2, 3, 4, 5, 6, 7, 8, 9 . z = \mathfrak{S}p + 4, 8, 12, 16, 1, 5, 9, 13$ und $17.$

Die 4 Reste 12, 16, 13 und 17 sind $> \frac{1}{2}p$, also ist $\varkappa = 4$ und *gerade*. $z^{\frac{1}{2}(p-1)}$ ist $42^9 = \mathfrak{S}p + 4^9 = \mathfrak{S}p + 64^3 = \mathfrak{S}p + 7^3 = \mathfrak{S}p + 343 = \mathfrak{S}p + 1$; gemäfs (4.).

Beweis. *A.* Man bezeichne diejenigen $\frac{1}{2}(p-1) - \varkappa$ Multiplicatoren von z in (1.), welche Reste $r < \frac{1}{2}p$ geben, durch m, die übrigen $\varkappa$ Multiplicatoren, welche Reste $> \frac{1}{2}p$ geben, durch μ. Für die letzteren Vielfachen von z nehme man die Quotienten *um 1 gröfser*, also statt der *positiven* echten Reste r die *negativen echten* Reste, welche nun durch ϱ bezeichnet werden mögen, so dafs also die Gleichungen (1.) zusammen folgende sind:

$$9. \quad \begin{cases} m_1 z = \mathfrak{S}p + r_1, \\ m_2 z = \mathfrak{S}p + r_2, \\ m_3 z = \mathfrak{S}p + r_3, \\ \dots \dots \dots \\ m_{\frac{1}{2}(p-1)-\varkappa} z = \mathfrak{S}p + r_{\frac{1}{2}(p-1)-\varkappa}; \end{cases} \qquad 10. \quad \begin{cases} \mu_1 z = \mathfrak{S}p - \varrho_1, \\ \mu_2 z = \mathfrak{S}p - \varrho_2, \\ \mu_3 z = \mathfrak{S}p - \varrho_3, \\ \dots \dots \dots \\ \mu_\varkappa z = \mathfrak{S}p - \varrho_\varkappa . \end{cases}$$

Alsdann sind zufolge (§. 35. 9.), da die Stammzahl p ungerade sein soll und zu jedem z theilerfremd ist, die r und ϱ in (9. u. 10.) zusammengenommen *alle die Zahlen*

11. $1, 2, 3, 4, \dots . \frac{1}{2}(p-1),$

und $\varkappa$ derselben sind *negativ*; während die m und μ *ebenfalls* alle die Zahlen (11.) sind.

B. Multiplicirt man also alle die $\frac{1}{2}(p-1)$ Gleichungen (9. u. 10.) in einander, so ergiebt sich

12. $1.2.3.4 \dots . \frac{1}{2}(p-1) z^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1.2.3.4 \dots . \frac{1}{2}(p-1)(-1)^\varkappa,$

und daraus folgt

13. $1.2.3.4 \dots . \frac{1}{2}(p-1)(z^{\frac{1}{2}(p-1)} - (-1)^\varkappa) = \mathfrak{S}p.$

Zufolge dieser Gleichung mufs das Product linkerhand mit p aufgehen. Es geht aber keiner der Factoren 1, 2, 3, 4, ... $\frac{1}{2}(p-1)$ des Productes mit p auf, weil alle $< p$ sind, also mufs der *letzte* Factor

$$14.\quad z^{\frac{1}{2}(p-1)} - (-1)^{\varkappa} = \mathfrak{S}p$$

sein (§. 25.), und daraus folgt

$$15.\quad z^{\frac{1}{2}(p-1)} = \mathfrak{S}p + (-1)^{\varkappa};$$

welches für ein *gerades* $\varkappa$ die Gleichung (3.) und für ein *ungerades* $\varkappa$ die Gleichung (4.) des Lehrsatzes giebt.

C. Hätte p Factoren > 1, so müfste wenigstens einer derselben $< \frac{1}{2}p$ sein, denn, alle $> \frac{1}{2}p$, würden eine Zahl $> p$ geben. Also geht dann in (13.) wenigstens ein Factor von p schon in $1.2.3.4 \ldots . \frac{1}{2}(p-1)$ auf, und die Gleichung (14.) folgt nicht mehr aus (13.). Der Lehrsatz gilt also nur *nothwendig,* wenn p eine *Stammzahl* ist.

Anm. *D.* Der Beweis beruht insbesondere auf dem Satze (§. 35.).

§. 42.

Lehrsatz.

Es seien p *und* q *zwei beliebige* ***Stammzahlen*** > 2, *die also immer durch*

$$1.\quad \mathrm{p} = 4\mathrm{n} \pm 1 \quad \text{und} \quad \mathrm{q} = 4\mathrm{m} \pm 1$$

ausgedrückt werden können (§. 28. IV.).

Man setze

$$2.\ \begin{cases} \mathrm{q} = \mu_1 \mathrm{p} + \mathrm{r}_1, \\ 2\mathrm{q} = \mu_2 \mathrm{p} + \mathrm{r}_2, \\ 3\mathrm{q} = \mu_3 \mathrm{p} + \mathrm{r}_3, \\ \ldots\ldots\ldots\ldots \\ \frac{1}{2}(\mathrm{p}-1)\mathrm{q} = \mu_{\frac{1}{2}(\mathrm{p}-1)} \mathrm{p} + \mathrm{r}_{\frac{1}{2}(\mathrm{p}-1)}; \end{cases} \quad \text{und} \quad 3.\ \begin{cases} \mathrm{p} = \nu_1 \mathrm{q} + \varrho_1, \\ 2\mathrm{p} = \nu_2 \mathrm{q} + \varrho_2, \\ 3\mathrm{p} = \nu_3 \mathrm{q} + \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \frac{1}{2}(\mathrm{q}-1)\mathrm{p} = \nu_{\frac{1}{2}(\mathrm{q}-1)} \mathrm{q} + \varrho_{\frac{1}{2}(\mathrm{q}-1)}; \end{cases}$$

und

$$4.\quad \mu_1 + \mu_2 + \mu_3 \ldots . + \mu_{\frac{1}{2}(\mathrm{p}-1)} = S\mu,$$

$$5.\quad \nu_1 + \nu_2 + \nu_3 \ldots . + \nu_{\frac{1}{2}(\mathrm{q}-1)} = S\nu.$$

Desgleichen bezeichne man

6. *die* ***Anzahl*** *der* $\mathrm{r} > \frac{1}{2}\mathrm{p}$ *in* (2.) *durch* k *und*

7. *die* ***Anzahl*** *der* $\varrho > \frac{1}{2}\mathrm{q}$ *in* (3.) *durch* $\varkappa$.

Alsdann findet folgendes Gesetz Statt:

Erstlich. *Sind nicht* p *und* q ***beide*** *von der Form* 4n — 1 *oder* 4m — 1, *und ist also*

$$8.\quad \begin{cases} 1.\ \textit{entweder}\ \ p = 4n+1, & q = 4m+1, \\ 2.\ \textit{oder}\ \ p = 4n+1, & q = 4m-1, \\ 3.\ \textit{oder}\ \ p = 4n-1, & q = 4m+1, \end{cases}$$

so ist

9. {
1. *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$ *und* $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q+1$, *und zwar wenn* $S\mu$ *oder wenn* k *gerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *gerade ist;*
2. *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1$ *und* $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q-1$, *und zwar wenn* $S\mu$ *oder wenn* k *ungerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *ungerade ist.*

Zweitens. Sind p *und* q *beide von der Form* $4n-1$ *oder* $4m-1$, *und ist also*

$$10.\quad p = 4n-1,\quad q = 4m-1,$$

so ist

11. {
1. *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$ *und* $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q-1$, *und zwar wenn* $S\mu$ *oder wenn* k *gerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *ungerade ist;*
2. *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1$ *und* $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q+1$, *und zwar wenn* $S\mu$ *oder wenn* k *ungerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *gerade ist.*

Dieses Gesetz wird Reciprocitätsgesetz für Stammzahlen genannt. Auf Deutsch wird es also Gegenseitigkeitsgesetz für Stammzahlen heifsen müssen. Das Gesetz findet nur für Stammzahlen, nicht nothwendig für andere Zahlen Statt, welche Theiler >1 *mit einander gemein haben.*

Man bezeichnet auch,

12. *dafs z. B.* $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q \pm 1$ *sei, durch* $\left(\frac{p}{q}\right) = \pm 1$.

Nach dieser Bezeichnung ist zufolge (9. u. 11.)

13. $\left(\frac{p}{q}\right) = +\left(\frac{q}{p}\right)$, *wenn* p *und* q *nicht beide von der Form* $4n-1$ *oder* $4m-1$ *sind, und*

14. $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *wenn* p *und* q *beide von der Form* $4n-1$ *oder* $4m-1$ *sind.*

Beispiel 1. Es sei

$$15.\quad p = 13,\quad q = 17,\quad \text{also}\ p = 4n+1,\quad q = 4m+1,$$

so ist in (2. u. 3.)

$$16.\left\{\begin{array}{lllll}
q=1p+4, & p=0q+13, & \text{also } S\mu=24, & q^1=\mathfrak{S}p+4, & p^1=\mathfrak{S}q+13,\\
2q=2p+8, & 2p=1q+9, & S\nu=24, & q^2=\mathfrak{S}p+3, & p^2=\mathfrak{S}q-1,\\
3q=3p+12, & 3p=2q+5, & k=4, & q^3=\mathfrak{S}p+9, & p^4=\mathfrak{S}q+1,\\
4q=5p+3, & 4p=3q+1, & \varkappa=4; & q^6=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+27, & p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1.\\
5q=6p+7, & 5p=3q+14, & & =\mathfrak{S}p+1; & \\
6q=7p+11; & 6p=4q+10, & & & \\
 & 7p=5q+7, & & & \\
 & 8p=6q+2 & & &
\end{array}\right.$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1$.
Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *gerade*.
Gemäfs (9. 1.).

Beispiel 2. Es sei

17. $p=13,\quad q=19,\quad$ also $\quad p=4n+1,\quad q=4m-1,$

so ist

$$18.\left\{\begin{array}{lllll}
q=1p+6, & p=0q+13, & \text{also } S\mu=27, & q^1=\mathfrak{S}p+6, & p^1=\mathfrak{S}q+13,\\
2q=2p+12, & 2p=1q+7, & S\nu=27, & q^2=\mathfrak{S}p+10, & p^2=\mathfrak{S}q-2,\\
3q=4p+5, & 3p=2q+1, & k=3, & q^4=\mathfrak{S}p+9, & p^4=\mathfrak{S}q+4,\\
4q=5p+11, & 4p=2q+14, & \varkappa=3; & q^6=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1; & p^8=\mathfrak{S}q-3,\\
5q=7p+4, & 5p=3q+8, & & & p^9=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.\\
6q=8p+10; & 6p=4q+2, & & & \\
 & 7p=4q+15, & & & \\
 & 8p=5q+9, & & & \\
 & 9p=6q+3; & & &
\end{array}\right.$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1$.
Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *ungerade*.
Gemäfs (9. 2.)

Beispiel 3. Es sei

19. $p=11,\quad q=17,\quad$ also $\quad p=4n-1,\quad q=4m+1,$

so ist

$$20.\left\{\begin{array}{lllll}
q=1p+6, & p=0q+11, & \text{also } S\mu=21, & q^1=\mathfrak{S}p+6, & p^1=\mathfrak{S}q+11,\\
2q=3p+1, & 2p=1q+5, & S\nu=19, & q^2=\mathfrak{S}p+3, & p^2=\mathfrak{S}q+2,\\
3q=4p+7, & 3p=1q+16, & k=3, & q^4=\mathfrak{S}p+9, & p^4=\mathfrak{S}q+4,\\
4q=6p+2, & 4p=2q+10, & \varkappa=4, & q^5=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1; & p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.\\
5q=7p+8; & 5p=3q+4, & & & \\
 & 6p=3q+15, & & & \\
 & 7p=4q+9, & & & \\
 & 8p=5q+3; & & &
\end{array}\right.$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1$.
Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *ungerade*.
Gemäfs (9. 2.).

Beispiel 4. Es sei

21. $p=7,\quad q=19,\quad$ also $\quad p=4n-1,\quad q=4m-1,$

so ist

$$22. \begin{cases} q=2p+5, & p=0q+7, \text{ also } S\mu=15, & q^1=\mathfrak{G}p+5, & p^1=\mathfrak{G}q+7, \\ 2q=5p+3, & 2p=0q+14, \quad S\nu=12, & q^2=\mathfrak{G}p+4, & p^2=\mathfrak{G}q+11, \\ 3q=8p+1; & 3p=1q+2, \quad k=1, & q^3=q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1, & p^4=\mathfrak{G}q+7, \\ & 4p=1q+9, \quad \varkappa=4; & & p^8=\mathfrak{G}q+11, \\ & 5p=1q+16, & & p^9=p^{\frac{1}{2}(q-1)}=\mathfrak{G}q+1. \\ & 6p=2q+4, & \multicolumn{3}{l}{\text{Also ist } q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1 \text{ und zugleich } p^{\frac{1}{2}(q-1)}=+1.} \\ & 7p=2q+11, & \multicolumn{3}{l}{\text{Desgleichen sind } S\mu \text{ und } k \text{ ungerade und } S\nu \text{ und } \varkappa \text{ gerade.}} \\ & 8p=2q+18, & \text{Gemäfs (11. 2.)} \\ & 9p=3q+6; \end{cases}$$

Erster Beweis. ***A.*** Zufolge (§. 38. 8.) ist für zwei ***beliebige ungerade*** Zahlen m und n, also auch hier für die ***ungeraden Stammzahlen*** p und q,

$$23. \quad S\mu+S\nu = \tfrac{1}{4}(p-1)(q-1).$$

Dieses giebt für die 3 Fälle (***Erstlich.*** 8.):

$$24. \begin{cases} 1. \quad S\mu+S\nu = \tfrac{1}{4}(4n)(4m) = 4mn = \text{einer geraden Zahl;} \\ 2. \quad S\mu+S\nu = \tfrac{1}{4}(4n)(4m-2) = 2n(m-1) = \text{einer geraden Zahl;} \\ 3. \quad S\mu+S\nu = \tfrac{1}{4}(4n-2)(4m) = 2m(n-1) = \text{einer geraden Zahl.} \end{cases}$$

Also ist in den Fällen (***Erstlich.***) des Lehrsatzes $S\mu+S\nu$ ***immer*** eine ***gerade*** Zahl, und folglich sind $S\mu$ und $S\nu$ immer ***zugleich*** gerade oder ***zugleich*** ungerade; wie es in (9.) behauptet wird.

Für den Fall (***Zweitens.*** 10.) dagegen giebt (23.)

$$25. \quad S\mu+S\nu = \tfrac{1}{4}(4n-2)(4m-2) = (2n-1)(2m-1)$$
$$= \text{einer } \textit{ungeraden} \text{ Zahl;}$$

also ist in dem Falle (***Zweitens.***) des Lehrsatzes $S\nu$ ***gerade,*** wenn $S\mu$ ***ungerade*** ist, und $S\nu$ ***ungerade,*** wenn $S\mu$ ***gerade*** ist.

B. Sodann ist nach (§. 39. 6.) in (2.) k gerade oder ungerade, je nachdem es $S\mu$ ist; denn so ist es zufolge (§. 39. 6.) für ***beliebige ungerade*** Zahlen u und v, also auch hier für die ungeraden Stammzahlen p und q. Nach (§. 41. 3. u. 4.) aber ist für eine beliebige Zahl z, die nicht mit p aufgeht, also auch hier für die Stammzahl q, $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p \pm 1$, je nachdem k ***gerade*** oder ***ungerade*** ist. Also ist hier

$$26. \begin{cases} q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1, \text{ wenn } S\mu \textit{ gerade} \text{ und} \\ q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1, \text{ wenn } S\mu \textit{ ungerade} \text{ ist.} \end{cases}$$

So wird es in (9. u. 11.) behauptet.

C. Aber in den Fällen (***Erstlich.***) sind $S\mu$ und $S\nu$ ***zugleich gerade*** und ***zugleich ungerade*** (***A.***): also ist in diesen Fällen auch ***zugleich,*** weil

$\varkappa$ und $S\nu$ eben so über $p^{\frac{1}{2}(q-1)}$, wie k und $S\mu$ über $q^{\frac{1}{2}(p-1)}$ entscheiden,

$$27.\quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1, \text{ wenn } S\mu \text{ oder } S\nu \textit{ gerade}, \text{ und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1, \text{ wenn } S\mu \text{ oder } S\nu \textit{ ungerade} \text{ ist.} \end{cases}$$

Dieses wird ferner in (9.) behauptet.

Dagegen ist in dem Falle (*Zweitens.*) $S\nu$ *ungerade*, wenn $S\mu$ *gerade* ist; und umgekehrt: also ist in diesem Falle

$$28.\quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1, \text{ wenn } S\mu \textit{ gerade}, \text{ also } S\nu \textit{ ungerade} \text{ und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1, \text{ wenn } S\mu \textit{ ungerade}, \text{ also } S\nu \textit{ gerade} \text{ ist.} \end{cases}$$

Dieses wird ferner in (11.) behauptet.

Zweiter Beweis. *D.* In (§. 36.) bezeichnet n_1 aus den mit v *aufgehenden* Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$29.\quad \begin{cases} v = \mathfrak{G}u + r_1, \\ 2v = \mathfrak{G}u + r_2, \\ 3v = \mathfrak{G}u + r_3, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \frac{1}{2}(u-1)v = \mathfrak{G}u + r_{\frac{1}{2}(u-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu u Reste $r > \frac{1}{2}u$ lassen, und n_8, aus den mit u *aufgehenden* Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$30.\quad \begin{cases} u = \mathfrak{G}v + \varrho_1, \\ 2u = \mathfrak{G}v + \varrho_2, \\ 3u = \mathfrak{G}v + \varrho_3, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \frac{1}{2}(v-1)u = \mathfrak{G}v + \varrho_{\frac{1}{2}(v-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu v Reste $\varrho > \frac{1}{2}v$ lassen.

Setzt man in (29. u. 30.) statt der dortigen, unter sich theilerfremden Zahlen u und v die gegenwärtigen, ebenfalls unter sich theilerfremden beiden Stammzahlen p und q, so sind die Gleichungen (29. u. 30.) diejenigen (2. u. 3.). Also ist für den gegenwärtigen Lehrsatz:

$$31.\quad n_1 = k \quad \text{und} \quad n_8 = \varkappa.$$

E. Nun ist zufolge (36. 16.)

$$32.\quad 2n_5 - n_1 - n_8 = \tfrac{1}{4}(u-1)(v-1),$$

also ist *hier*

$$33.\quad 2n_5 - (k+\varkappa) = \tfrac{1}{4}(p-1)(q-1).$$

Aber $\frac{1}{4}(p-1)(q-1)$ ist in den Fällen (*Erstlich.* 8.), wie aus (24.) erhellet, *immer gerade;* und nur in dem Falle (*Zweitens.* 10.) *ungerade.* Die Zahl $2n_5$, welche sie auch sein mag, ist *immer gerade*, also ist vermöge (33.)

34. $\begin{cases} k+\varkappa \text{ in den Fällen } (\textit{Erstlich. } 8.) \text{ immer } \textit{gerade}, \text{ und} \\ k+\varkappa \text{ nur in dem Falle } (\textit{Zweitens. } 10.) \textit{ ungerade}; \end{cases}$

woraus folgt, dafs

35. $\begin{cases} k \text{ und } \varkappa \text{ in den Fällen } (\textit{Erstlich. } 8.) \text{ beide zugleich } \textit{gerade} \text{ oder } \textit{ungerade} \text{ sind und dafs} \\ k \text{ und } \varkappa \text{ in dem Falle } (\textit{Zweitens. } 10.), \text{ das eine } \textit{gerade}, \text{ das andere } \textit{ungerade} \text{ ist.} \end{cases}$

F. Zufolge (§. 41. 3. u. 4.) ist, da das dortige $\varkappa$ für $z=q$ hier k und für $z=p$ und $p=q$ hier $\varkappa$ ist,

36. $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$, wenn k, und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q+1$, wenn $\varkappa$ *gerade* ist und

37. $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1$, wenn k, und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q-1$, wenn $\varkappa$ *ungerade* ist;

also finden in den Fällen (*Erstlich.* 8.) vermöge (35.) die Gleichungen (36.) oder die Gleichungen (37.) *zugleich* Statt, und in dem Falle (*Zweitens.* 10.) findet die erste Gleichung (36.) mit der zweiten (37.), oder die zweite (36.) mit der ersten (37.) *zugleich* Statt; und zwar auf die Weise, wie es (9. u. 11.) aussagen.

G. Dafs $S\mu$ und k und $S\nu$ und $\varkappa$ *zugleich gerade* oder *ungerade* sind, wie es (9. u. 11.) noch behaupten, folgt bei diesem zweiten Beweise aus (§. 39. 6.).

H. Dafs der Lehrsatz *nur* für Stammzahlen p und q, nicht nothwendig für andere Zahlen, welche Theiler >1 gemein haben, Statt findet, folgt daraus, dafs der Satz (§. 41.), auf welchem er mit beruht, *nur* für *Stammzahlen* nothwendig gilt.

Anm. *I.* Der erste Beweis beruft sich auf die Lehrsätze (§. 38. 39. und 41.), der zweite auf die Lehrsätze (§. 36., 39. und 41.); der erste also auf den Satz (§. 38.) von den *Quotienten* μ in den Gleichungen $((1, 2, 3, 4, \ldots \frac{1}{2}n$ oder $\frac{1}{2}(n-1))m = \mu n + r$, der zweite auf den Satz (§. 36.) von den *Resten* der Zahlen $1, 2, 3, 4, \ldots \frac{1}{2}(uv-1)$, dividirt durch u und v; aufserdem auf *dieselben* Sätze (§. 39. u. 41.). Die Sätze (§. 36., 38., 39. u. 41.) *bereiten* das Reciprocitäts- oder Gegenseitigkeitsgesetz für Stammzahlen *vor.* Sie sind aber von ihm getrennt und besonders aufgestellt worden, theils um den Beweis des gegenwärtigen Satzes an sich zu verkürzen und dadurch übersichtlicher zu machen, theils weil die vorbereitenden Sätze auch für sich selbst noch andere Anwendungen finden.

Das Reciprocitäts- oder Gegenseitigkeitsgesetz findet wieder in der gesammten Theorie der Zahlen vielfache weitere Anwendungen und ist daher, gleich dem *Fermat*sche Satze (§. 40.), ebenfalls als einer der Hauptsätze der Zahlenlehre zu betrachten.

§. 43.

Erklärung.

In den gewöhnlichen algebraischen Gleichungen von der Form

1. $\varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots + \varepsilon_1 x + \varepsilon_0 = 0,$

wo der Exponent n eine *ganze positive* Zahl ist und die ε beliebige Zahlgröfsen sind, kann bekanntlich x nur n von einander verschiedene, positive oder negative, reelle oder imaginäre *Werthe* haben, und diese Werthe von x nennt man *Wurzeln* der Gleichung.

In der Theorie der Zahlen kommen Gleichungen vor, die ganz dieselbe *Form* wie die algebraischen (1.) haben, nur dafs zu dem letzten Gliede noch ein *unbestimmtes* Vielfache irgend einer *bestimmten* Zahl z hinzugethan oder davon hinweggenommen ist, während zugleich alle Coëfficienten ε positive oder negative *ganze* Zahlen sind: Gleichungen also, welche die Form

2. $\varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots + \varepsilon_1 x + \varepsilon_0 = \mathfrak{S} z$

haben Solche Gleichungen drücken, wie man sieht, aus, dafs das *Polynom* oder die *Potenzenreihe* linkerhand mit der bestimmten Zahl z *aufgehe.* Für solche Gleichungen kommt es dann insbesondere auf diejenigen positiven oder negativen *ganzzahligen* Werthe von x an, welche die eben genannte Bedingung erfüllen, oder welche der Gleichung (2.) *genugthun.* Diese ganzzahligen Werthe von x nennt man ebenfalls *Wurzeln* der Gleichung (2.). Sie sollten zwar, bestimmter, *ganzzahlige Wurzeln* der Gleichung heifsen, aber da in der Zahlentheorie überhaupt nur von *ganzen* Zahlen die Rede ist, so kann das Beiwort *ganzzahlig* auch füglich wegbleiben und man kann die der Gleichung (2.) genugthuenden ganzzahligen Werthe von x blofs *Wurzeln* nennen. Gleichungen wie (2.) kann man dagegen, wenn man will, zum Unterschiede von den gewöhnlichen algebraischen Gleichungen, wie (1.), *Zahlengleichungen* nennen.

§. 44.

Lehrsatz.

I. *Die Zahlengleichung*

1. $f_n x = \varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_2 x^2 + \varepsilon_1 x + \varepsilon_0 = \mathfrak{S} p,$

in welcher der Zeiger n *an* f *den Grad des Polynoms oder der Potenzenreihe* $\varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_0$ *bezeichnet, kann, wenn* p *eine Stammzahl ist, und* ε_n *und* ε_0 *gehen nicht mit* p *auf, nicht mehr*

als n *positive ganzzahlige Wurzeln* $x > 0$ *und* $< p$ *haben; gleichviel ob andere von den* ε *als* ε_n *und* ε_0 *mit p aufgehen, oder nicht.*

II. *Gehen die ersten* $\varkappa$ *Coëfficienten* $\varepsilon_n, \varepsilon_{n-1}, \varepsilon_{n-2}, \ldots \varepsilon_{n-\varkappa+1}$ *mit* p *auf, der nächste Coëfficient* $\varepsilon_{n-\varkappa}$, *nebst* ε_0 *aber nicht, so kann die Gleichung* (1.) *nicht mehr als* $n-\varkappa$ *positive ganzzahlige Wurzeln* > 0 *und* $< p$ *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

III. *Gehen die letzten* λ *Coëfficienten* $\varepsilon_{\lambda-1}, \varepsilon_{\lambda-2}, \varepsilon_{\lambda-3}, \ldots \varepsilon_0$ *mit* p *auf, der nächst vorige Coëfficient* ε_λ *nebst* ε_n *aber nicht, so hat die Gleichung* (1.) *zunächst nothwendig* p *zur Wurzel; aufserdem aber kann sie nicht mehr als* $n-\lambda$ *positive ganzzahlige Wurzeln* > 0 *und* $< p$ *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

IV. *Gehen die ersten* $\varkappa$ *und die letzten* λ *Coëfficienten* (II. u. III.) *mit* p *auf, der nächste Coëfficient* $\varepsilon_{n-\varkappa}$ *links und der nächste Coëfficient* ε_λ *rechts aber nicht, so hat die Gleichung* (1.) *erst nothwendig* p *zur Wurzel; aufserdem kann sie nicht mehr als* $n-\varkappa-\lambda$ *positive ganzzahlige Wurzeln* > 0 *und* $< p$ *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

V. *Jedesmal hat die Gleichung* (1.) *auch noch eben so viele negative ganzzahlige Wurzeln, deren Werth zeichenfrei* > 0 *und* $< p$ *ist, als sie positive Wurzeln hat. Diese negativen Wurzeln finden sich, wenn man von den positiven Wurzeln* p *abzieht.*

VI. *Nur dann, wenn alle Coëfficienten* ε *einzeln mit* p *aufgehen, kann die Gleichung* (1.) *mehr als* n *positive und* n *negative ganzzahlige Wurzeln haben, deren Werthe zeichenfrei* > 0 *und* $< p$ *sind; und zwar hat sie dann nothwendig alle die Zahlen* $\pm(1, 2, 3, 4, \ldots p-1)$ *zu Wurzeln.*

VII. *Keinesweges aber hat die Gleichung* (1.) *nothwendig immer* n *positive und* n *negative Wurzeln* > 0 *und* $< p$. *Sie kann deren auch weniger, und selbst gar keine haben.*

VIII. *Ist* $n = p$, *oder* $> p$, *so kann die Gleichung* (1.) *alle die Zahlen* $\pm(1, 2, 3, 4, \ldots p-1)$ *zu Wurzeln haben; jedoch auch nicht alle, und selbst keine derselben.*

IX. *Soll* $f_n x$ *auch nur für einen mehr als* n *Werthe von* $x > 0$ *und* $< p$ *mit* p *aufgehen: soll also die Gleichung* (1.) *auch nur für einen*

mehr als n *solcher Werthe von* x *erfüllt werden, so ist dies nicht anders möglich, als dafs alle die Coëfficienten* ε *einzeln mit* p *aufgehen.*

X. *Wenn die Gleichung* (1.) *nicht* n, *sondern nur* $k < n$ *Wurzeln* > 0 *und* $< p$ *hat, also das Polynom* $f_n x$ *nur für* k *Werthe von* x > 0 *und* $< p$ *aufgeht, so läfst sich die Gleichung* $f_n x = \mathfrak{G} p$ (1.) *immer auf die Form*

$$2. \quad f_n x = (x - e_1)(x - e_2)(x - e_3) \ldots (x - e_k) f_{n-k} x = \mathfrak{G} p$$

bringen, wo e, e_1, e_3, ... e_k *die* k *Werthe* > 0 *und* $< p$ *sind, für welche* $f_n x$ *mit* p *aufgeht,* $f_{n-k} x$ *aber ein Polynom vom Grade* $n - k$ *ist, welches* ε_n *zum Coëfficienten seines ersten Gliedes, also* $\varepsilon_n x^{n-k}$ *zum ersten Gliede hat und, insofern* $n - k > 1$, *für keinen der andern Werthe von* x *mit* p *aufgeht.*

Auch pafst der Ausdruck (2.) *von* $f_n x$ *gleichmäfsig auf den Fall, wenn die Gleichung* (1.) n *Wurzeln hat oder* $f_n x$ *für* n *Werthe von* x > 0 *und* $< p$ *mit* p *aufgeht. Es ist alsdann* $k = n$; *in* (2.) *ist* $f_{n-k} x = \varepsilon_n$ *und der Ausdruck von* (1.) *also alsdann*

$$3. \quad f_n x = (x - e_1)(x - e_2)(x - e_3) \ldots (x - e_n) \varepsilon_n = \mathfrak{G} p.$$

XI. *Wenn in* (1.) ε_n *nicht mit* p *aufgeht, aber auch nur dann, läfst sich die Gleichung* (1.), *wenn das Polynom für* k *Werthe von* x > 0 *und* $< p$ *mit* p *aufgeht, immer auf eine andere*

$$4. \quad f_n x = (x^k - \delta_{k-1} x^{k-1} + \delta_{k-2} x^{k-2} - \delta_{k-3} x^{k-3} \ldots \mp \delta_2 x^2 \pm \delta_1 x \mp \delta_0) f_{n-k} x = \mathfrak{G} p$$

bringen, in welcher das erste Glied des Polynoms vom Grade k, 1 *zum Coëfficienten hat, das erste Glied des für keinen Werth von* x *mit* p *aufgehenden Factors* $f_{n-k} x$, $\varepsilon_n x^{n-k}$ *ist, und die* δ *der Reihe nach die Summen der Producte der* k *Werthe* e_1, e_2, e_3, ... e_k *von* $x > 0 < p$ *zu einem, zweien, dreien etc. bis* k *sind, für welche* $f_n x$ *mit* p *aufgeht.*

In dem Fall, wo $f_n x$ *für* n *Werthe von* $x > 0$ *und* $< p$ *mit* p *aufgeht, läfst sich die Gleichung* (1.) *auf die Form*

$$5. \quad f_n x = (x^n - \delta_{n-1} x^{n-1} + \delta_{n-2} x^{n-2} - \delta_{n-3} x^{n-3} \ldots \mp \delta_2 x^2 \pm \delta_1 x \mp \delta_0) \varepsilon_n = \mathfrak{G} p$$

bringen, wo wiederum das erste Glied des Polynoms vom Grade n, 1 *zum Coëfficienten hat und die* δ *der Reihe nach die Summen der Producte der* n *Werthe* e_1, e_2, e_3, ... e_n *von* $x > 0 < p$ *zu einem, zweien, dreien etc. bis* n *sind, für welche* $f_n x$ *mit* p *aufgeht.*

Immer gehen die Producte $(x - e_1)(x - e_2)(x - e_3) \ldots (x - e_k)$ *in* (2.) *und* $(x - e_1)(x - e_2)(x - e_3) \ldots (x - e_n)$ *in* (3.), *ersteres für die nemlichen*

k, *letzteres für die nemlichen* n *Werthe von* x *mit* p *auf, wie das Polynom* $f_n x$ *selbst. Und eben so verhält es sich mit den Polynomen von den Graden* k *und* n *in* (4. und 5.).

XII. *Wenn ein Polynom* $f_n x$ *für* n—1 *Werthe von* $x > 0 < p$ *aufgeht, so geht es auch noch für einen* n*ten Werth von* $x > 0 < p$ *mit* p *auf, der aber nicht nothwendig von einem der Werthe* $e_1, e_2, e_3, \ldots e_{n-1}$ *verschieden ist.*

Beispiele. *a.* 1. Die Gleichung

$$6. \quad x^3 + 2x^2 + x - 4 = \mathfrak{G}.11,$$

für welche $n = 3$, $p = 11$ ist, hat $n = 3$ positive und eben so viele negative Wurzeln. Jene sind $+1$, $+3$ und $+5$, diese -1, -8 und -6. Denn für alle diese Werthe von x geht $x^3 + 2x^2 + x - 4$ mit $p = 11$ auf.

2. Die Gleichung

$$7. \quad 2x^4 - 5x^3 - 26x^2 + 4x - 9 = \mathfrak{G}.7,$$

für welche $n = 4$, $p = 7$ ist, hat nur die $k = 2$ positiven Wurzeln 4 und 5 und die $k = 2$ negativen Wurzeln -3 und -2. Für keinen andern Werth von $x < p = 7$ geht $2x^4 - 5x^3 - 26x^2 + 4x - 9$ mit $p = 7$ auf.

3. Die Gleichung

$$8. \quad 3x^3 - 16x^2 + 25x + 58 = \mathfrak{G}.7,$$

für welche $n = 3$, $p = 7$ ist, hat wieder die $n = 3$ positiven Wurzeln $+1$, $+3$ und $+6$ und die $n = 3$ negativen Wurzeln -6, -4 und -1.

4. Die Gleichung

$$9. \quad 4x^3 - 8x^2 - 2x + 9 = \mathfrak{G}.7$$

hat *gar keine* ganzzahligen Wurzeln.

5. Die Gleichung

$$10. \quad x^6 - 1 = \mathfrak{G}.7$$

hat alle die Zahlen $\pm(1, 2, 3, 4, 5 \text{ und } 6 = (p-1))$ zu Wurzeln.

b. Die Gleichung (7.) ist das Nemliche wie

$$11. \quad (x-4)(x-5)(2x^2 + 13x + 51) = \mathfrak{G}.7 - 203x + 1029$$
$$= 7(\mathfrak{G} - 29x + 147) = \mathfrak{G}.7,$$

wo der Factor $f_2 x = 2x^2 + 13x + 51$ für *keinen* Werth $> 0 < p$ von x mit p aufgeht und das erste Glied dieses Factors $2x^2 = \varepsilon_n x^{n-k}$ ist; gemäfs (2.).

Die Gleichung (8.) ist das Nemliche wie

$$12. \quad (x-1)(x-3)(x-6).3 = \mathfrak{G}.7 - 14x^2 + 56x + 112$$
$$= 7(\mathfrak{G} + 2x^2 + 8x + 16) = \mathfrak{G}.7,$$

wo der Factor 3 von $(x-1)(x-3)(x-6)$ gleich ε_n ist; gemäfs (3.).

c. Die Ausdrücke (11.) und (12.) sind so viel als

13. $(x^2-9x+20)(2x^2+13x+51) = \mathfrak{G}.7$ und

14. $(x^3-10x^2+27x-18).3 = \mathfrak{G}.7.$

In (13.) ist, mit (4.) verglichen, $\delta_{k-1}=9=4+5$, $\delta_{k-2}=\delta_0=20=4.5$. In (14.) ist, mit (5.) verglichen, $\delta_{n-1}=10=1+3+6$, $\delta_{n-2}=27=1.3+1.6+3.6$ und $\delta_{n-3}=\delta_0=18=1.3.6$; gemäfs (X.).

Beweis. *A.* Es werde das Polynom $f_n x$ durch das ***Binom*** $x-e_1$ ***dividirt***, so wird das erste Glied des Quotienten $\varepsilon_n x^{n-1}$, und der Quotient wird ein Polynom vom Grade $n-1$ sein, also durch $f_{n-1}x$ bezeichnet werden können; der ***Rest*** der Division, welcher r_1 sein mag, wird ***gar kein*** x enthalten, weil man mit der Division so lange fortfahren kann, als ein Glied des Rests noch x enthält. Die Division giebt nemlich Folgendes:

15.
$$\begin{array}{l} x-e_1 \mid \varepsilon_n x^n + \varepsilon_{n-1}x^{n-1}+\varepsilon_{n-2}x^{n-2}+\varepsilon_{n-3}x^{n-3}\dots+\varepsilon_1 x+\varepsilon_0 \mid \varepsilon_n x^{n-1}+(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-2} \\ \qquad -\varepsilon_n x^n+e_1\varepsilon_n x^{n-1} \qquad\qquad\qquad\qquad\qquad\qquad +(\varepsilon_{n-2}+e_1\varepsilon_{n-1}+e_1^2\varepsilon_n)x^{n-3}\dots \\ \hline \qquad (\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-1}+\varepsilon_{n-2}x^{n-2}+\varepsilon_{n-3}x^{n-3}\dots+\varepsilon_1 x+\varepsilon_0 \\ \qquad -(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-1}+e_1(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-2} \\ \hline \qquad\qquad (\varepsilon_{n-2}+e_1\varepsilon_{n-1}+e_1^2\varepsilon_n)x^{n-2}+\varepsilon_{n-3}x^{n-3}\dots+\varepsilon_1 x+x_0 \end{array}$$

Und so weiter.

Man wird also setzen können:

16. $f_n x = (x-e_1)f_{n-1}x+r_1$,

wo von $f_{n-1}x$ das ***erste*** Glied $\varepsilon_n x^{n-1}$ ist und r_1 ***kein*** x enthält.

B. Das Polynom $f_{n-1}x$ in (16.) vom Grade $n-1$ werde nun von neuem durch ein anderes ***Binom*** $x-e_2$ dividirt, so wird man aus ganz gleichen Gründen setzen können:

17. $f_{n-1}x = (x-e_2)f_{n-2}x+r_2$,

wo das ***erste*** Glied von $f_{n-2}x$ wieder $\varepsilon_n x^{n-2}$ ist und r_2 ***kein*** x enthält.

Ferner wird man setzen können, wenn weiter das Polynom $f_{n-2}x$ vom Grade $n-2$ in (17.) mit einem dritten ***Binom*** $x-e_3$ dividirt wird:

18. $f_{n-2}x = (x-e_3)f_{n-3}x+r_3$,

wo von $f_{n-3}x$ das ***erste Glied*** $\varepsilon_n x^{n-3}$ ist und r_3 kein x enthält.

Und so weiter; zuletzt also

19. $f_1 x = (x-e_n)f_0 x+r_n$,

wo das ***erste Glied*** von $f_0 x$, das heifst $f_0 x$ selbst ist, weil $f_0 x$ vom Grade 0 ist, also ***nur ein*** Glied hat und nur $x^0=1$ vorkommt, $=\varepsilon_n x^0=\varepsilon_n$ ist und r_n kein x enthält.

C. Es sind nemlich, wie aus (15.) zu sehen, die Polynome $f_{n-1}x$, $f_{n-2}x$, $f_{n-3}x$, ... der Reihe nach von der Form

$$20. \quad \begin{cases} f_{n-1}x = \varepsilon_n x^{n-1} + \overset{1}{\varepsilon}_{n-2} x^{n-2} + \overset{1}{\varepsilon}_{n-3} x^{n-3} \dots + \overset{1}{\varepsilon}_1 x + \overset{1}{\varepsilon}_0, \\ f_{n-2}x = \varepsilon_n x^{n-2} + \overset{2}{\varepsilon}_{n-3} x^{n-3} + \overset{2}{\varepsilon}_{n-4} x^{n-4} \dots + \overset{2}{\varepsilon}_1 x + \overset{2}{\varepsilon}_0, \\ f_{n-3}x = \varepsilon_n x^{n-3} + \overset{3}{\varepsilon}_{n-4} x^{n-4} + \overset{3}{\varepsilon}_{n-5} x^{n-5} \dots + \overset{3}{\varepsilon}_1 x + \overset{3}{\varepsilon}_0, \\ \dots\dots\dots\dots \end{cases}$$

Geht man also damit bis zum vorletzten Polynom vom Grade $n-(n-1)=1$ fort, so wird solches die Form

$$21. \quad f_1 x = \varepsilon_n x + \overset{n-1}{\varepsilon_0}$$

bekommen, und dieses, mit dem letzten Binom $x-e_n$ dividirt, giebt

$$22. \quad f_1 x = \varepsilon_n (x-e_n) + \varepsilon_n e_n + \overset{n-1}{\varepsilon_0},$$

welches, mit (19.) verglichen,

$$23. \quad f_0 x = \varepsilon_n \text{ und}$$

$$24. \quad \varepsilon_n e_n + \overset{n-1}{\varepsilon_0} = r_n$$

giebt; letzteres ohne x.

D. Substituirt man nun zunächst (17.) in (16.), so ergiebt sich

$$25. \quad f_n x = (x-e_1)(x-e_2) f_{n-2} x + (x-e_1) r_2 + r_1.$$

Substituirt man hierin (18.), so erhält man

$$26. \quad f_n x = (x-e_1)(x-e_2)(x-e_3) f_{n-3} x + (x-e_1)(x-e_2) r_3 + (x-e_1) r_2 + r_1,$$

u. s. w.; zuletzt, da $f_0 = \varepsilon_n$ ist,

$$27. \quad \begin{aligned} f_n x = {} & (x-e_1)(x-e_2)(x-e_3)\dots(x-e_n)\varepsilon_n \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-1}) r_n \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-2}) r_{n-1} \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-3}) r_{n-2} \\ & \dots\dots\dots\dots \\ & + (x-e_1)(x-e_2) r_3 \\ & + (x-e_1) r_2 \\ & + r_1. \end{aligned}$$

E. Ist nun e_1 einer der *ganzzahligen positiven* Werthe von $x < p$ und > 0, welche der Gleichung (1.) genugthun, so giebt der Ausdruck von $f_n x$ (27.) für $x = e_1$, da alle Glieder rechts bis auf das letzte $x - e_1$ zum Factor haben und also für $x = e_1$ verschwinden,

$$28. \quad f_n e_1 = r_1;$$

und da nun zugleich gemäfs (1.) $f_n e_1 = \mathfrak{G}p$ sein soll,

$$29.\quad r_1 = \mathfrak{G}p.$$

F. Ist e_2 ein zweiter der ***ganzzahligen positiven*** Werthe von x >0 und $<p$, welche der Gleichung (1.) genugthun, so giebt der Ausdruck (27.) für $x=e_2$, da alle Glieder rechts bis auf die beiden letzten $x-e_2$ zum Factor haben und also für $x=e_2$ verschwinden,

$$30.\quad f_n e_2 = (e_2-e_1)r_2+r_1,$$

und da $f_n e_2$ gemäfs (1.) $=\mathfrak{G}p$ sein soll und r_1 nach (29.) schon $=\mathfrak{G}p$ ist,

$$31.\quad (e_2-e_1)r_2 = \mathfrak{G}p.$$

Nun sind aber e_1 und e_2 beide $<p$ und positiv, also ist auch der zeichenfreie Werth von $e_2-e<p$, und folglich geht e_2-e_1 ***nicht*** mit p auf. Daher mufs, vermöge (31.) und (§. 25.), r_2 mit p aufgehen und folglich

$$32.\quad r_2 = \mathfrak{G}p$$

sein.

G. Ist e_3 ein dritter der ***ganzzahligen positiven*** Werthe von x >0 und $<p$, welche der Gleichung (1.) genugthun, so giebt der Ausdruck (27.) für $x=e_3$, da alle Glieder rechts bis auf die drei letzten für $x=e_3$ verschwinden,

$$33.\quad f_n e_3 = (e_3-e_1)(e_3-e_2)r_3+(e_3-e_1)r_2+r_1,$$

und da $f_n e_3$ gemäfs (1.) $=\mathfrak{G}p$ sein soll und r_1 und r_2 gemäfs (29. und 32.) ebenfalls $=\mathfrak{G}p$ sind,

$$34.\quad (e_3-e_1)(e_3-e_2)r_3 = \mathfrak{G}p.$$

Hier geht wieder weder e_3-e_1 noch e_3-e_2 mit p auf, weil e_1, e_2, e_3 sämmtlich $<p$ und positiv sind: also mufs r_3 mit p aufgehen und folglich

$$35.\quad r_3 = \mathfrak{G}p \text{ sein.}$$

So findet sich weiter $r_4=\mathfrak{G}p$, $r_5=\mathfrak{G}p$ etc., und zusammen

$$36.\quad r_1,\ r_2,\ r_3,\ r_4,\ \ldots\ r_n = \mathfrak{G}p,$$

wenn e_1, e_2, e_3, ... e_n, n verschiedene ganzzahlige Werthe von $x>0$ und $<p$ sind, die der Gleichung (1.) genugthun.

H. Da nun die Gleichung (27.) für ***jeden beliebigen*** Werth von x, so wie für ***beliebige*** Werthe der e Statt findet, indem der Ausdruck von $f_n x$ rechts eine blofse, durch die wiederholte Division entstandene ***identisch*** verwandelte Form von $f_n x$ ist, wo, wie sich so eben fand, ***in dem Fall*** wo die e die n verschiedenen Werthe von x, >0 und $<p$ bezeichnen, für welche $f_n x$ mit p der Voraussetzung nach ***aufgeht***, die sämmtlichen r gleich $\mathfrak{G}p$ sein ***müssen***, so giebt die Gleichung (27.) für diesen Fall:

37. $f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots(x-e_n)\varepsilon_n + \mathfrak{G}p$,

für ***jeden beliebigen*** Werth von x.

I. Hieraus folgt nun, dafs $f_n x$ für ***nicht mehr*** als n Werthe von x, die >0 und $<p$ sind, mit p aufgehen kann, insofern nicht ε_n mit p aufgeht. Denn gesetzt es sei zu den n Werthen $e_1, e_2, e_3, \ldots e_n$ von x, >0 und $<p$, für welche $f_n x$ nach der Voraussetzung mit p aufgeht, k noch ein $n+1$ter solcher Werth, also $f_n k = \mathfrak{G}p$, so müfste vermöge (37.)

38. $(k-e_1)(k-e_2)(k-e_3)\ldots(k-e_n)\varepsilon_n = \mathfrak{G}p$

sein. Dies aber ist nicht möglich, da $e_1, e_2, e_3, \ldots e_n$ und k sämmtlich >0 und $<p$ sein sollen, also auch die zeichenfrei genommenen Werthe aller der Factoren $k-e_1$, $k-e_2$, $k-k_3$, ... $k-e_k$, $<p$ sind, desgleichen ε_n nach der Voraussetzung nicht mit p aufgeht. Also ist es in dem so eben genannten Fall von ε_n nicht möglich, dafs $f_n x$ für ***mehr*** als n Werthe von x, die >0 und $<p$ sind, mit p aufgehe, oder dafs die Gleichung (1.) in diesem Falle mehr als n positive ganzzahlige Wurzeln >0 und $<p$ habe. Und zwar ist es gleichgültig, ob die Coëfficienten $\varepsilon_{n-1}, \varepsilon_{n-2}, \varepsilon_{n-3}, \ldots \varepsilon_1$ mit p aufgehen, oder nicht; denn sie kommen in der Gleichung (24.), aus welcher das Nicht-Stattfinden von mehr als n positiven Wurzeln der Gleichung (1.) folgt, nicht vor. Dieses zusammen ist was (I.) behauptet.

K. Geht ε_n mit p ***auf***, so ist $\varepsilon_n x^n = \mathfrak{G}p$, für ***jeden*** Werth von x. Eben so sind, wenn etwa weiter $\varepsilon_{n-1}, \varepsilon_{n-2}, \varepsilon_{n-3}$ u. s. w. bis $\varepsilon_{n-\varkappa+1}$ mit p aufgehen, und dann zunächst $\varepsilon_{n-\varkappa}$ ***nicht***, auch alle die Glieder $\varepsilon_{n-1}x^{n-1}$, $\varepsilon_{n-2}x^{n-2}$, $\varepsilon_{n-3}x^{n-3}$, ... $\varepsilon_{n-\varkappa+1}x^{n-\varkappa+1}$ gleich $\mathfrak{G}p$; was auch x sein mag. Also reducirt sich die Gleichung (1.) in diesem Fall auf

39. $\varepsilon_{n-\varkappa}x^{n-\varkappa} + \varepsilon_{n-\varkappa-1}x^{n-\varkappa-1} + \varepsilon_{n-\varkappa-2}x^{n-\varkappa-2}\ldots + \varepsilon_1 x + \varepsilon_0 = \mathfrak{G}p$;

und diese Gleichung kann nach (I.) ***nicht mehr*** als $n-\varkappa$ positive ganzzahlige Wurzeln >0 und $<p$ haben, gleichviel ob andere von den auf $\varepsilon_{n-\varkappa}$ ***folgenden*** Coëfficienten, den letzten ausgenommen, mit p aufgehen, oder nicht. Gemäfs (II.).

L. Gehen $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots \varepsilon_{\lambda-1}$ mit p auf, so sind alle die Glieder ε_0, $\varepsilon_1 x$, $\varepsilon_2 x^2$, $\varepsilon_3 x^3$, ... $\varepsilon_{\lambda-1}x^{\lambda-1}$ gleich $\mathfrak{G}p$; was auch x sein mag. Also reducirt sich die Gleichung (1.) in diesem Fall auf

$\varepsilon_n x^n + \varepsilon_{n-1}x^{n-1} + \varepsilon_{n-2}x^{n-2}\ldots + \varepsilon_\lambda x^\lambda = \mathfrak{G}p$ oder

40. $x^\lambda(\varepsilon_n x^{n-\lambda} + \varepsilon_{n-1}x^{n-\lambda-1} + \varepsilon_{n-2}x^{n-\lambda-2}\ldots + \varepsilon_{\lambda+1}x + \varepsilon_\lambda) = \mathfrak{G}p$.

Dieser Gleichung wird offenbar zunächst für $x=p$ genuggethan; sodann aber kann der Factor zu x^λ zufolge (I.) für ***nicht mehr*** als $n-\lambda$ Werthe von x,

> 0 und $< p$, mit p aufgehen. Also kann die Gleichung (1.) in solchem Falle nur $n-\lambda$ solcher Wurzeln haben, während sie aufserdem ***nothwendig*** p selbst zur Wurzel hat. Gemäfs (III.). Zugleich folgt hieraus, dafs es für (I.) eine ***Bedingung*** ist, dafs der letzte Coëfficient ε_0 ***nicht*** mit p aufgehe; denn ist dies der Fall, so modificirt sich (I.) nach (III.).

M. Gehen die ersten $\varkappa$ und die letzten λ Coëfficienten ε mit p auf, so sind alle die Glieder, in welchen sich diese Coëfficienten befinden, gleich $\mathfrak{S}p$; was auch x sein mag. Also reducirt sich die Gleichung in diesem Fall auf

$$\varepsilon_{n-\varkappa}x^{n-\varkappa}+\varepsilon_{n-\varkappa-1}x^{n-\varkappa-1}+\varepsilon_{n-\varkappa-2}x^{n-\varkappa-2}\ldots\ldots+\varepsilon_\lambda x^\lambda=\mathfrak{S}p \text{ oder}$$

41. $$x^\lambda(\varepsilon_{n-\varkappa}x^{n-\varkappa-\lambda}+\varepsilon_{n-\varkappa-1}x^{n-\varkappa-\lambda-1}+\varepsilon_{n-\varkappa-2}x^{n-\varkappa-\lambda-2}\ldots\ldots+\varepsilon_{\lambda+1}x+\varepsilon_\lambda)=\mathfrak{S}p.$$

Dieser Gleichung wird wieder zunächst für $x=p$ genuggethan; sodann aber kann der Factor zu x^λ zufolge (I.) für ***nicht mehr*** als $n-\varkappa-\lambda$ Werthe von x, > 0 und $< p$, mit p aufgehen. Also kann die Gleichung (1.) in dem gegenwärtigen Falle nur $n-\varkappa-\lambda$ solcher Wurzeln haben, während sie aufserdem ***nothwendig*** p selbst zur Wurzel hat. Gemäfs (IV.).

N. Wenn $f_n x$ (1.) für $x=e$ mit p aufgeht, so geht es auch nothwendig für $x=e-p$ mit p auf. Denn $x=e-p$ ist so viel als $x=\mathfrak{S}p+e$, und zufolge (§. 11. 20.) ist alsdann, für jeden beliebigen ganzzahligen positiven Exponenten τ,

42. $$x^\tau=\mathfrak{S}p+e^\tau;$$

also giebt (1.), wenn man darin $e-p$ statt x setzt, vermöge (29.),

$$f_n(e-p)=\mathfrak{S}p+\varepsilon_n e^n+\varepsilon_{n-1}e^{n-1}+\varepsilon_{n-2}e^{n-2}\ldots\ldots+\varepsilon_2 e^2+\varepsilon_1 e+\varepsilon_0 \text{ oder}$$

43. $$f_n(e-p)=\mathfrak{S}p+f_n e.$$

Ist also $f_n e=\mathfrak{S}p$, so ist es auch $f_n(e-p)$, und folglich gehört zu ***jeder positiven*** ganzzahligen Wurzel $e > 0$ und $< p$, welche die Gleichung (1.) hat, auch eine ***negative*** ganzzahlige Wurzel $e-p$, deren zeichenfreier Werth ebenfalls > 0 und $< p$ ist. Gemäfs (V.).

O. Gehen ***alle*** Coëfficienten ε in (1.) einzeln mit p auf, so ist ***jedes*** Glied von $f_n x$ gleich $\mathfrak{S}p$ und folglich die ***ganze*** Potenzenreihe $f_n x=\mathfrak{S}p$; und dieser Gleichung thut ***jeder beliebige*** Werth von x ein Genüge. Also hat alsdann die Gleichung (1) alle die Zahlen $\pm(1, 2, 3, 4, \ldots\ldots p-1)$, deren absoluten Werthe > 0 und $< p$ sind, zu Wurzeln. Jedoch ist es so auch ***nur*** in dem vorausgesetzten Fall; sind nicht ***alle*** ε gleich $\mathfrak{S}p$, so verhält es sich nach den verschiedenen Umständen gemäfs (I. II. III. oder IV.). Dieses behauptet (VI.).

P. Um nachzuweisen, dafs zufolge (VII.) die Gleichung (1.) auch *weniger* als n ganzzahlige Wurzeln >0 und $<p$ haben kann, darf nur gezeigt werden, dafs es in *irgend einem* Falle sich so verhalte. Auf einen solchen Fall führt der Fermatsche Lehrsatz (§. 40.). Diesem Satze zufolge nemlich hat die Gleichung

$$44.\quad x^{p-1} - 1 = \mathfrak{G}p$$

alle die Zahlen $1, 2, 3, 4, \ldots p-1$ zu Wurzeln. *Eben deshalb* aber hat z. B. die Gleichung

$$45.\quad x^{p-1} - 2 = \mathfrak{G}p \quad \text{oder} \quad x^{p-1} - 1 - 1 = \mathfrak{G}p$$

keine der Zahlen $1, 2, 3, 4, \ldots p-1$ zu Wurzeln, und folglich *gar keine* Wurzeln; denn da $x^{p-1} - 1$ für $x = 1, 2, 3, 4, \ldots p-1$ mit p aufgeht, und 1 *nicht*, so geht $x^{p-1} - 1 - 1$ oder $x^{p-1} - 2$ für *keine* der Werthe $1, 2, 3, \ldots p-1$ von x mit p auf, und folglich hat (32.) *gar keine* Wurzeln.

Q. Der Beweis von (I.) ändert sich nicht, wenn auch $n = p$ oder $> p$ ist. Also könnte in diesem Fall die Gleichung (1.) n verschiedene Wurzeln >0 und $<p$ haben. Aber es *giebt nur* die $p-1$ Zahlen $1, 2, 3, \ldots p-1$, welche >0 und $<p$ sind; also kann die Gleichung (1.) in solchem Fall alle die Zahlen $\pm(1, 2, 3, 4, \ldots p-1)$ zu Wurzeln haben; wiewohl auch nicht alle, und selbst keine derselben. Gemäfs (VIII.).

R. Wenn $f_n x$ für n verschiedene Werthe von $x > 0 < p$ aufgeht, so verwandelt sich $f_n x$ zufolge (*H.*) in den Ausdruck (37.). Derselbe kann zufolge (*I.* 38.) nicht anders für einen $n+1$ten Werth von x mit p aufgehen, als wenn ε_n mit p aufgeht. Also mufs, schon wenn $f_n x$ auch nur für einen mehr als die n Werthe $e_1, e_2, e_3, \ldots e_n$ von x mit p aufgehen soll, nothwendig ε_n mit p aufgehen.

Geht nun aber ε_n mit p auf, so ist das *erste Glied* $\varepsilon_n x^n$ von $f_n x$ (1.) selbst $= \mathfrak{G}p$ und das Polynom $f_n x$ reducirt sich auf ein anderes $\varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_0$ vom $n-1$ten Grade. Dieses kann schon selbst für n Werthe, und um so mehr für $n+1$ Werthe von x, aus *demselben* Grunde nicht anders mit p aufgehen, als wenn ε_{n-1} mit p aufgeht. Dadurch, dafs ε_{n-1} mit p aufgehen mufs, reducirt sich dann das Polynom weiter auf ein anderes $\varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots + \varepsilon_0$ vom $n-2$ten Grade; und hier mufs wieder $\varepsilon_{n-2} = \mathfrak{G}p$ sein u. s. w.; bis zu $\varepsilon_0 = \mathfrak{G}p$. Also müssen, wie es (IX.) behauptet, wenn $f_n x$ für mehr als n Werthe von $x > 0 < p$ mit p aufgehen soll, alle die Coëfficienten ε in (1.) einzeln mit p aufgehen.

S. Um zu beweisen was (X.) behauptet, dividire man zuerst, eben

wie in (15.), $f_n x$ durch $x-e_1$, hierauf, wie dort in (16.), $f_{n-1}x$ durch $x-e_2$, $f_{n-2}x$ wie in (17.) durch $x-e_3$ u. s. w., fahre aber damit nicht wie in (*B.* und *C.*) bis zu $x-e_n$ fort, so dafs die letzte Gleichung nicht die (19.) ist, sondern nur bis zu $x-e_k$, so dafs die letzte Gleichung

$$46.\quad f_{n-k+1}\,x = (x-e_k)f_{n-k}\,x + r_k$$

ist, wo indessen immer wie in (16, 17, 18.) das erste Glied von $f_{n-k}x$ $\varepsilon_n x^{n-k}$ ist und r_k *kein* x enthält.

T. Substituirt man nun wieder erst (17.) in (16.), in das Resultat (18.), u. s. w., so wird man, ähnlich dem Ausdruck (27.), für welchen $k=3$ sein würde,

$$\begin{aligned}47.\quad f_n x = {} & (x-e_1)(x-e_2)(x-e_3)\dots(x-e_k)f_{n-k}x\\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-1})r_k\\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-2})r_{k-1}\\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-3})r_{k-2}\\ & \dots\dots\dots\dots\dots\dots\\ & +(x-e_1)(x-e_2)r_3\\ & +(x-e_1)r_2\\ & +r_1\end{aligned}$$

erhalten.

U. Ist nun e_1 einer der ganzzahligen positiven Werthe von $x>0$ $<p$, welche der Gleichung (1.) genugthun, so giebt (47.), für $x=e_1$,

$$48.\quad f_n x_1 = r_1,$$

und da $f_n e_1 = \mathfrak{G}p$ sein soll,

$$49.\quad r_1 = \mathfrak{G}p.$$

Ist e_2 ein zweiter Werth von x, für welchen $f_n e_2 = \mathfrak{G}p$ ist, so giebt (47.) für $x=e_2$

$$50.\quad f_n e_2 = (e_2-e_1)r_2 + r_1 = \mathfrak{G}p,$$

oder, da r_1 schon $=\mathfrak{G}p$ ist (49.),

$$51.\quad (e_2-e_1)r_2 = \mathfrak{G}p,$$

und da e_2-e_1 mit p *nicht* aufgeht (*F.*),

$$52.\quad r_2 = \mathfrak{G}p.$$

Ist e_3 ein dritter Werth von x, für welchen $f_n x_3 = \mathfrak{G}p$ ist, so giebt (47.) für $x=e_3$

$$53.\quad f_n e_3 = (e_3-e_1)(e_2-1)r_3 + (e_3-e_1)x_2 + r_1 = \mathfrak{G}p,$$

oder, da r_1 und r_2 schon $=\mathfrak{G}p$ sind (49. und 52.),

$$54.\quad (e_3-e_1)(e_2-e_1)r_3 = \mathfrak{G}p,$$

also, da $e_3 - e_1$ und $e_2 - e_1$ *nicht* mit p aufgehn,

$$55. \quad r_3 = \mathfrak{G}p.$$

Und so weiter.

So findet man aus (47.), bis zu r_k, dafs

$$56. \quad r_1,\ r_2,\ r_3,\ \ldots.\ r_k = \mathfrak{G}p$$

und also vermöge (47.)

$$57. \quad f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots.(x-e_k)f_{n-k}x + \mathfrak{G}p$$

ist.

V. Hier geht rechterhand die Gröfse $(x-e_1)(x-e_2)\ldots.(x-e_k)f_{n-k}x$ offenbar für $x = e_1, e_2, e_3, \ldots. e_k$ mit p auf, eben wie es von $f_n x$ selbst vorausgesetzt wird; denn für jeden dieser Werthe von x ist sie $=0$. Also ist im Fall $f_n x$ für $x = e_1, e_2, e_3, \ldots. e_k$ mit p aufgeht:

58. $(x-e_1)(x-e_2)(x-e_3)\ldots.(x-e_k)f_{n-k}x = \mathfrak{G}p$, gemäfs (2.), eben wie es $f_n x = \mathfrak{G}p$ ist (1.); und auf diese Form kann also in solchem Fall die Gleichung (1.) gebracht werden.

Das erste Glied von $f_{n-k}x$ ist $\varepsilon_n x^{n-k}$, gemäfs (*S.*); auch kann $f_{n-k}x$, insofern $n-k>1$ ist, für keinen andern Werth von x mehr mit p aufgehen, denn sonst müfste vermöge (57.) $f_n x$ selbst für einen solchen Werth von x mit p aufgehen, gegen die Voraussetzung; gemäfs (IX.).

W. Der Ausdruck (3.) in (X.) geht unmittelbar aus (2.) oder (58.) hervor, wenn man $k=n$ setzt, und pafst auf den Fall, wenn $f_n x$ für n Werthe von $x > 0 < p$ mit p aufgeht.

X. Zufolge (§. 2.) ist

$$59. \quad (1+a)(1+b)(1+c)\ldots.(1+k) = 1+P_1+P_2+P_3\ldots.+P_k,$$

wenn man durch P_1, P_2, P_3, ... P_k die Summe aller möglichen Producte der Gröfsen a, b, c, ... k zu einer, zwei, drei etc. bis k bezeichnet.

Man setze in (59.)

$$60. \quad a = -\frac{e_1}{x},\quad b = -\frac{e_2}{x},\quad c = -\frac{e_3}{x},\quad \ldots.\quad k = -\frac{e_k}{x}$$

und multiplicire (59.) rechts und links mit x^k, so erhält man

$$x^k\left(1-\frac{e_1}{x}\right)\left(1-\frac{e_2}{x}\right)\left(1-\frac{e_1}{x}\right)\ldots.\left(1-\frac{e_k}{x}\right) = x^k(1+P_1+P_2+P_3\ldots.+P_k)$$

oder

$$61. \quad (x-e_1)(x-e_2)(x-e_3)\ldots.(x-e_k) = x^k + x^kP_1 + x^kP_2 + x^kP_3\ldots. + x^kP_k.$$

Hier bedeuten die P die Summen aller möglichen Producte von $-\frac{e_1}{x}$, $-\frac{e_2}{x}$, $-\frac{e_3}{x}$, ... $-\frac{e_k}{x}$ zu einem, zwei, drei etc., bis k. Die Producte dieser

sämmtlich *negativen* Gröfsen werden vom ersten ab abwechselnd negativ und positiv sein und der Reihe nach x, x^2, x^3, ... x^k im Nenner enthalten. Es werden also die P, wenn man der Reihe nach die Summen aller möglichen Producte der Gröfsen e_1, e_2, e_3, ... e_k selbst, wie in (X. zu 4.), durch δ_{k-1}, δ_{k-2}, δ_{k-3}, ... δ_0 bezeichnet, folgende Werthe haben:

62. $$P_1 = -\frac{\delta_{k-1}}{x},\quad P_2 = -\frac{\delta_{k-2}}{x^2},\quad P_3 = -\frac{\delta_{k-3}}{x^3},\quad \dots\dots\quad P_k = -\frac{\delta_0}{x^k}.$$

Diese Ausdrücke in (61.) gesetzt, giebt

63. $$(x-e_1)(x-e_2)(x-e_3)\dots\dots(x-e_k)$$
$$= x^k - \delta_{k-1}x^{k-1} + \delta_{k-2}x^{k-2} - \delta_{k-3}x^{k-3}\dots\dots \pm \delta_0,$$

und dies weiter in (2.) substituirt, giebt den Ausdruck (4.) des Lehrsatzes.

Der Ausdruck (5.) geht unmittelbar aus (4.) hervor, für $k = n$.

Y. Wenn $f_n x$ für $k = n-1$ Werthe von $x > 0 < p$ aufgeht, so ist in seinem Ausdrucke (2.) $n-k = 1$, also $f_{n-k}x$ von der Form $\varepsilon_n x + \beta$, oder, wenn man $\varepsilon_n = \mathfrak{G}p + a$ und $\beta = \mathfrak{G}p + b$ setzt, von der Form $(\mathfrak{G}p + a)x + \mathfrak{G}p + b = \mathfrak{G}p + ax + b$, wo a und $b > 0 < p$ sind. Und $ax + b$ geht *immer* für irgend ein $x > 0 < p$ mit p auf. Denn zu $ax + b = \mathfrak{G}p$ gehört, da ε_n, und folglich a zu p theilerfremd ist, immer nach (§. 34.) *ein* solcher Werth von $x > 0 < p$. Also geht $f_{n-k}x$ immer noch für irgend einen Werth von $x > 0 < p$, der aber nicht nothwendig von e_1, e_2, e_3, ... e_{n-1} verschieden ist, mit p auf, und folglich auch in (2.) $f_n x$; gemäfs (XII.).

Z. Der gegenwärtige Lehrsatz findet wieder vielfältige weitere Anwendungen und ist daher wieder einer der Hauptlehrsätze der Zahlentheorie.

§. 45.

Lehrsatz.

Wenn in der Gleichung

1. $$(\mathrm{m}p + \mathrm{z})^2 = \mathfrak{G}p + \mathrm{r}$$

p ***eine ungerade Stammzahl*** > 2 ***ist und man giebt dem positiven oder negativen*** z ***die zeichenfreien Werthe***

2. $$1,\ 2,\ 3,\ 4,\ \dots\dots\ p-1,$$

so dafs $\mathrm{m}p + \mathrm{z}$, ***mit beliebigem ganzzahligem*** m, ***alle möglichen positiven oder negativen, mit*** p ***nicht aufgehenden ganzen Zahlen ausdrückt, so durchläuft***

I. ***wenn man für ein gleiches*** m ***der Reihe nach***

3. $$\mathrm{z} = +1,\ +2,\ +3,\ +4,\ \dots\dots\ +p-1,$$
4. $$\mathrm{z} = -1,\ -2,\ -3,\ -4,\ \dots\dots\ -(p-1)$$

setzt, der absolute Werth von r *in* (1.) *niemals etwa ebenfalls alle die Zahlen* (2.), *sondern immer nur die Hälfte derselben, und immer die nemlichen, was auch* m *sein mag; die andere Hälfte der Zahlen* (2.) *wird von* r *für das gleiche* p *niemals berührt. Auch geben schon*

5. $z = \pm 1, \pm 2, \pm 3, \ldots \pm \frac{1}{2}(p-1)$

alle Werthe von r *welche Statt finden; die folgenden*

6. $z \pm \frac{1}{2}(p-1)+1, \frac{1}{2}(p-1)+2, \frac{1}{2}(p-1)+3, \ldots\ldots p-1$

geben dieselben r, *und zwar in entgegengesetzter Aufeinanderfolge. Desgleichen geben positive und negative* z *von gleichen absoluten Werthen gleiche* r.

II. *Da in* (1.) r *nichts anders ist als der Rest, welcher bleibt, wenn man das Quadrat* $(mp+z)^2$ *mit* p *dividirt, so ist* r *ein Rest zu einem Quadrat oder ein Quadratrest. Und da nun nach* (1.) *die Hälfte der Zahlen* (2.) *von* r *berührt wird, so sind diese Hälfte der Zahlen* (2.) *Quadratreste zu* p; *die andere Hälfte, welche* r *nicht berührt, sind nicht Reste von Quadraten, also Nicht-Quadratreste zu* p.

III. *Da man die Gleichung* (1.) *auch, mit einem ganz beliebigen positiven oder negativen ganzzahligen* n, *wie folgt schreiben kann:*

7. $(mp+z)^2 = \mathfrak{S}p+(np+r) = \mathfrak{S}p+R,$

indem nur $\mathfrak{S}$ *in* (7.) *um* n *kleiner sein darf, als in* (1.), *so kann in* (7.) *auch*

8. $np+r = R$

als der Rest der Division des Quadrats $(mp+z)^2$ *durch* p *betrachtet werden, und folglich als Quadratrest zu* p. *Da aber* n *ganz beliebig ist, so kann die Zahl* R *positiv oder negativ und so grofs oder so klein gemacht werden, als man will. Und da nun* r *nach* (I.) *immer nur die Hälfte der Zahlen* (2.) *berührt, so giebt es überhaupt eben so viele mit* p *nicht aufgehende Zahlen, die durch* R (6.) *ausgedrückt werden, als dergleichen Zahlen, die* R *nicht ausdrückt.*

In Folge dessen ist denn jede mögliche positive oder negative ganze, grofse oder kleine, nicht mit p *aufgehende Zahl entweder Quadratrest oder Nichtquadratrest zu* p, *und für jedes* n *sind eben so viele Zahlen Quadratreste, als andere Nichtquadratreste.*

Die R *für* $n = 0$, *oder die* r, *deren absolute Werthe unter den Zahlen* (2.) *sich befinden, und die also* > 0 *und* $< p$ *sind, könnte man zum Unterschiede von den gröfsern oder kleinern* R *positive oder negative echte Quadratreste und die Hälfte der Zahlen* (2.), *welche von* (2.)

nicht berührt werden, positive oder negative **echte Nichtquadratreste** *nennen.*

Beispiel 1. Es sei

$$9.\quad p=7,$$

so ist in (7.) der Reihe nach für $m=0,1,2,3,\dots$, $n=0,1,2,3,\dots$ und $z=\pm(1,2,3,\dots)$

$$10.\quad \left\{\begin{array}{rlll}
(0p\pm1)^2 & =+\,0p+1 & =-\,1p+\,8 & =-\,2p+15\dots\\
 & =+\,1p-6 & =+\,2p-13 & =+\,3p-20\dots\\
(0p\pm2)^2 & =+\,0p+4 & =-\,1p+11 & =-\,2p+18\dots\\
 & =+\,1p-3 & =+\,2p-10 & =+\,3p-17\dots\\
(0p\pm3)^2 & =+\,1p+2 & =-\,0p+\,9 & =-\,1p+16\dots\\
 & =+\,2p-5 & =+\,3p-12 & =+\,4p-19\dots\\
(0p\pm4)^2 & =+\,2p+2 & =+\,1p+\,9 & =+\,0p+16\dots\\
 & =+\,3p-5 & =+\,4p-12 & =+\,5p-19\dots\\
(0p\pm5)^2 & =+\,3p+4 & =+\,2p+11 & =+\,1p+18\dots\\
 & =+\,4p-3 & =+\,5p-10 & =+\,6p-17\dots\\
(0p\pm6)^2 & =+\,5p+1 & =+\,4p+\,8 & =+\,3p+15\dots\\
 & =+\,6p-6 & =+\,7p-13 & =+\,8p-20\dots\\
(\pm1p\pm1)^2 & =+\,9p+1 & =+\,8p+\,8 & =+\,7p+15\dots\\
 & =+10p-6 & =+19p-13 & =+12p-20\dots\\
(\pm1p\pm2)^2 & =+11p+4 & =+10p+11 & =+\,9p+18\dots\\
 & =-12p-3 & =+11p-10 & =+10p-17\dots\\
\dots & \dots & \dots & \dots
\end{array}\right.$$

Die *positiven echten* Quadratreste sind hier 1, 4, 2, die *negativen echten* Quadratreste —6, —3 und —5, und die einen und die andern ergeben sich schon aus $z=\pm(1,2,3)$, also aus der *ersten Hälfte* der Werthe von $z=\pm(1,2,3,4,5,6)$. Dieselben positiven und negativen echten Reste kehren für $(\pm1p\pm z)^2$, $(\pm2p\pm z)^2$ etc. immer wieder. Die Zahlen 3, 5 und 6 aus (2.) werden hier von den positiven echten Resten und die Zahlen 1, 2 und 4 von den negativen echten Resten nicht berührt. Erstere sind also die *positiven echten Nichtquadratreste*, letztere die *negativen echten Nichtquadratreste* zu $p=7$. Überhaupt sind

$$11.\quad \left.\begin{array}{l}\text{die positiven Zahlen } +(1,2,4,\ 8,\ 9,11,15,16,18,\dots)\\ \text{und die negativen Zahlen } -(3,5,6,10,12,13,17,19,20,\dots)\end{array}\right\}\ \textit{Quadratreste}\ \text{zu } p=7 \text{ und}$$

$$12.\quad \left.\begin{array}{l}\text{die positiven Zahlen } +(3,5,6,10,12,13,17,19,20,\dots)\\ \text{und die negativen Zahlen } -(1,2,4,\ 8,\ 9,11,15,16,18,\dots)\end{array}\right\}\ \textit{Nichtquadratreste}\ \text{zu } p=7.$$

2. Da es insbesondere auf die *echten* positiven und negativen Quadratreste und Nichtquadratreste ankommt, so setzen wir dieselben vorläufig für einige der ersten ungeraden Stammzahlen >2 hierher. Die echten positiven und die negativen echten Quadratreste bezeichnen wir durch $\pm r$, und die echten positiven und negativen Nichtquadratreste durch $\pm \varrho$.

Für $p=3$ ist $+r=+1, \quad +\varrho=+2,$
$-r=-2, \quad -\varrho=-1;$
Für $p=5$ ist $+r=+(1,4), \quad +\varrho=+(2,3),$
$-r=-(1,4), \quad -\varrho=-(2,3);$
Für $p=7$ ist $+r=+(1,2,4), \quad +\varrho=+(3,5,6),$
$-r=-(3,5,6), \quad -\varrho=-(1,2,4);$
Für $p=11$ ist $+r=+(1,3,4,5,9), \quad +\varrho=+(2,6,7,8,10);$
$-r=-(2,6,7,8,10), \quad -\varrho=-(1,3,4,5,9);$
Für $p=13$ ist $+r=+(1,3,4,9,10,12), \quad +\varrho=+(2,5,6,7,8,11),$
$-r=-(1,3,4,9,10,12), \quad -\varrho=-(2,5,6,7,8,11);$
Für $p=17$ ist $+r=+(1,2,4,8,9,13,15,16),$
$+\varrho=+(3,5,6,7,10,11,12,14),$
$-r=-(1,2,4,8,9,13,15,16),$
$-\varrho=-(3,5,6,7,10,11,12,14);$
Für $p=19$ ist $+r=+(1,4,5,6,7,9,11,16,17),$
13. $+\varrho=+(2,3,8,10,12,13,14,15,18),$
$-r=-(2,3,8,10,12,13,14,15,18),$
$-\varrho=-(1,4,5,6,7,9,11,16,17);$
Für $p=23$ ist $+r=+(1,2,3,4,6,8,9,12,13,16,18),$
$+\varrho=+(5,7,10,11,14,15,17,19,20,21,22),$
$-r=-(5,7,10,11,14,15,17,19,20,21,22),$
$-\varrho=-(1,2,3,4,6,8,9,12,13,16,18);$
Für $p=29$ ist $+r=+(1,4,5,6,7,9,13,16,20,22,23,24,25,28),$
$+\varrho=+(2,3,8,10,11,12,14,15,17,18,19,21,26,27),$
$-r=-(1,4,5,6,7,9,13,16,20,22,23,24,25,28),$
$-\varrho=-(2,3,8,10,11,12,14,15,17,18,19,21,26,27);$
Für $p=31$ ist $+r=+(1,2,4,5,7,8,9,10,14,16,18,19,20,25,28),$
$+\varrho=+(3,6,11,12,13,15,17,21,22,23,24,26,27,29,30),$
$-r=-(3,6,11,12,13,15,17,21,22,23,24,26,27,29,30),$
$-\varrho=-(1,2,4,5,7,8,9,10,14,16,18,19,20,25,28);$
. .

Beweis *A*. Es ist $(-z)^2 = +z^2$. Also geben positive und negative z von gleichem absolutem Werthe *gleiche* Reste r.

B. Es ist $(p-z)^2 = p^2 - 2pz + z^2 = \mathfrak{G}p + z^2$, also ist

14. wenn $z^2 = \mathfrak{G}p + r$ ist, auch $(p-z)^2 = \mathfrak{G}p + r$.

Also geben z^2 und $(p-z)^2$ *gleiche* Reste r. Setzt man daher

15. $z = \pm(1, 2, 3, \ldots \tfrac{1}{2}(p-1)$,

so geben sie *denselben* Rest r wie

16. $z = \pm(p-1, p-2, p-3, \ldots \tfrac{1}{2}(p+1))$,

und folglich giebt schon die *erste Hälfte* der Zahlen $\pm(1, 2, 3, \ldots p-1)$ *alle* Quadratreste r; die *zweite Hälfte* giebt *dieselben* Reste, und zwar in *umgekehrter* Aufeinanderfolge: denn $p-1$ giebt denselben Rest wie 1, $p-2$ denselben Rest wie 2 u. s. w.

Dieses zusammen ist was in (I.) behauptet wird. Das Übrige ist an sich klar.

Anm. *C*. Die Benennungen *quadratische und nichtquadratische Reste zu* p, welche man hie und da auch findet, dürfte grammatisch weniger richtig sein als *Quadratreste* und *Nichtquadratreste,* welches geradezu ausdrückt, was gemeint ist; denn jene Benennung würde Reste bezeichnen, die *selber Quadrate* oder nicht Quadrate, oder doch quadratischer oder nicht quadratischer Art sind; was hier nicht der Fall ist, indem die r keineswegs *immer Quadrate,* und eben so wenig die Zahlen, welche r nicht berührt, nothwendig immer *nicht Quadrate* sind.

§. 46.

Erklärung.

Zwei ganze Zahlen z_1 und z_2, deren Product, durch eine dritte ganze Zahl a dividirt, den Rest r giebt, so dafs

1. $z_1 z_2 = \mathfrak{G}a + r$

ist, nennt man, wenn mehrere solcher Zahlenpaare zu *demselben* Divisor a *denselben* Rest r geben, *correspondirende* oder auch *conjugirte* Zahlen.

Da die Zahlen z_1 und z_2 in (1.) nichts anders sind als Factoren von $\mathfrak{G}a +$ dem Rest r, oder einfacher, ein *Factorenpaar für r zu a,* so könnten sie auch füglich *so heifsen.* Will man indessen eine andere, nicht unmittelbar bezeichnende, sondern nur mehr andeutende Benennung, so könnte man die Zahlen z_1 und z_2 *auf Deutsch zusammengehörige Zahlen* nennen; doch müfste dann der Unterscheidung wegen eigentlich noch hinzugesetzt werden „für r zu a.“

§. 47.

Lehrsatz.

I. *Wenn* p *eine ungerade Stammzahl ist, so sind alle die Zahlen*

$$1. \quad z = 2, 3, 4, 5, \dots p-2$$

je zu zweien Factorenpaare von 1 *zu* a (*zusammengehörige Zahlen für* 1 *zu* p §. 46.), *so dafs in*

$$2. \quad z_1 z_2 = \mathfrak{G}p + 1$$

z_1 *und* z_2 *alle die Zahlen* (1.) *sein können. Und zwar ist in* (2.) *für keins der* z, (1.) z_1 *gleich* z_2. *Auch gehört zu jedem* z_1 *nur ein* z_2, *so dafs in* (2.) z_1 *und* z_2 *jeden der Werthe von* z (1.) *nur einmal haben können. Die Anzahl der Factorenpaare ist* $\frac{1}{2}(p-3)$.

II. *Die beiden von den Zahlen* $< p$ *noch übrigen Zahlen* 1 *und* $p-1$ *geben mit keinem der* z (1.), *sondern nur mit sich selbst multiplicirt* $\mathfrak{G}p+1$, *und mit einander multiplicirt,*

$$3. \quad 1.(p-1) = \mathfrak{G}p - 1.$$

III. *Wenn in*

$$4. \quad z_1 z_2 = \mathfrak{G}p + \varrho$$

ϱ *ein positiver Nichtquadratrest* (§. 45. II.) *ist, so sind alle Zahlen* $< p$, *also alle die Zahlen*

$$5. \quad z = 1, 2, 3, 4, \dots p-1$$

je zu zweien Factorenpaare von ϱ *zu* p (*zusammengehörige Zahlen für* ϱ *zu* p §. 46.), *so dafs in*

$$6. \quad z_1 z_2 = \mathfrak{G}p + \varrho$$

z_1 *und* z_2 *alle die Zahlen* (5.) *sein können. Und zwar kann wieder in* (6.) *für kein* z (5.) z_1 *gleich* z_2 *sein. Auch gehört zu jedem* z_1 *nur ein* z_2, *so dafs in* (6.) z_1 *und* z_2 *jeden der Werthe von* z (5.) *nur einmal haben können. Die Anzahl der Factorenpaare ist hier* $\frac{1}{2}(p-1)$.

Beispiel. Zu I. und II. Es sei $p = 13$, so sind 2.7; 3.9; 4.10; 5.8 und 6.11 sämmtlich $= \mathfrak{G}p+1$. Keiner der Factoren in diesen $\frac{1}{2}(p-3)$ $= 5$ Producten ist dem andern *gleich;* keiner kommt mehr als einmal vor, und die Factoren durchlaufen *alle* die Zahlen 2, 3, 4, 5, 6, 7, 8, 9, 10 und $11 = p - 2$ (1.); gemäfs (I.). Die Gleichung (3.) in (II.) ist an sich klar.

Zu III. Einer der *Nichtquadratreste* zu $p = 13$ ist $\varrho = 8$ (§. 45. 13.), und die Producte 1.8; 2.4; 3.7; 5.12; 6.10; 9.11 sind sämmtlich $= \mathfrak{G}p + 8$.

Keiner der Factoren in diesen $\frac{1}{2}(p-1)=6$ Producten ist dem andern *gleich*; keiner kommt mehr als einmal vor, und die Factoren durchlaufen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 und $12=p-1$ (5.); gemäfs (III.).

Beweis von I. *A.* Wenn man irgend ein z_1 aus den z (1.) mit allen den Zahlen 1, 2, 3, 4, ... $p-1$ multiplicirt und die Producte durch p dividirt, so durchlaufen die *Reste* nach (§. 34. I.) *alle* die Zahlen 1, 2, 3, 4, ... $p-1$, indem *jedes* z (1.) zu p *theilerfremd* ist. Also mufs auch irgend ein z_2 aus den Zahlen 1, 2, 3, 4, ... $p-1$

$$7.\quad z_1 z_2 = \mathfrak{G}p+1$$

geben. Und dies für *jedes* $z_1=2, 3, 4, \dots p-2$ (1.).

B. Das z_2 zu einem *bestimmten* z_1 kann aber nicht *gleich* z_1 sein; denn sonst wären $z_1^2=\mathfrak{G}p+1$ oder $z_1^2-1=\mathfrak{G}p$ oder

$$8.\quad (z_1-1)(z_1+1) = \mathfrak{G}p$$

und es müfste entweder z_1-1 oder z_1+1 mit p aufgehen; was nicht der Fall ist, da $z_1-1<p$, und auch, da z_1 nicht gröfser als $p-2$ sein soll (1.) $z_1+1<p$ ist.

C. Ferner kann z_2 weder 1 noch $p-1$ sein; denn $z_1.1$ giebt z_1 und $z_1(p-1)$ giebt $\mathfrak{G}p-1$, also beides nicht $\mathfrak{G}p+1$; wie es sein soll. Also kann z_2 nur eine der Zahlen (1.) sein.

D. Auch kann *nur ein* z aus (1.), für ein *bestimmtes* z_1, $z_1 z_2=\mathfrak{G}p+1$ geben; dann gäbe noch ein anderes z, z. B. z_3, $z_1 z_3=\mathfrak{G}p+1$, so wäre

$$9.\quad z_1(z_2-z_3) = \mathfrak{G}p$$

und es müfste also entweder z_1 oder z_2-z_3 mit p *aufgehen;* was nicht sein kann, da z_1 und z_2-z_3 beide $<p$ sind.

E. Wegen (*D.*) gehört nun zu jedem *andern* z_1 auch ein *anderes* z_2, denn sonst gehörten zu demselben z_2 zwei verschiedene z_1; was nach (*D.*) nicht sein kann; und folglich kann weder *dasselbe* z_1, noch *dasselbe* z_2, mehr als einmal vorkommen, so lange man nemlich für z_1 Zahlen nimmt, die nicht schon z_2 berührten.

Geschieht *dieses*, so ist das zugehörige z_2 wieder das z_1, welches $z_1 z_2=\mathfrak{G}p+1$ gab; so dafs also, wenn man z_1 *alle* die Zahlen (1.) durchlaufen läfst, jedes Product *zweimal* vorkommt und folglich die *Anzahl* der Producte $\frac{1}{2}(p-3)$ ist, da $p-3$ Zahlen z in (1.) vorhanden sind. In diesen $\frac{1}{2}(p-3)$ Producten kommt aber dann kein z aus (1.) zweimal vor, während zugleich die z (1.) *alle* vorkommen.

Dieses zusammen ist was (I.) behauptet.

Von II. *F.* Was (II.) behauptet ist an sich klar.

Von III. *G* Wenn man irgend ein z_1 aus den z (5.) mit allen den Zahlen 1, 2, 3, 4, ... $p-1$ multiplicirt und die Producte durch p dividirt, so durchlaufen wieder die ***Reste*** nach (§. 34. I.) *alle* die Zahlen 1, 2, 3, 4, ... $p-1$, indem jedes z (5.) zu p *theilerfremd* ist. Also berühren die Reste auch *alle Nichtquadratreste* ϱ zu p, und folglich mufs irgend ein z_2 aus den Zahlen 1, 2, 3, 4, ... $p-1$ auch

$$10. \quad z_1 z_2 = \mathfrak{G}p + \varrho$$

geben, wo ϱ ein *bestimmter Nichtquadratrest* ist.

H. Dieses z_2 kann nicht *gleich* z_1 sein; denn sonst wäre

$$11. \quad z_1^2 = \mathfrak{G}p + \varrho,$$

und ϱ wäre ein *Quadratrest*, nicht ein *Nichtquadratrest.*

I. Ferner kann *nicht mehr als ein* z aus (5.) für ein bestimmtes z_1, $z_1 z_2 = \mathfrak{G}p + \varrho$ geben; denn gäbe noch ein anderes z, z. B. z_3, $z_1 z_3 = \mathfrak{G}p + \varrho$, so wäre

$$12. \quad z_1(z_2 - z_3) = \mathfrak{G}p,$$

was, wie in (*D.*), nicht sein kann.

K. Wegen (*I.*) gehört wieder zu jedem *andern* z_1 auch ein *anderes* z; denn sonst würden zu demselben z_2 zwei verschiedene z_1 gehören; was nach (*I.*) nicht sein kann. Folglich kann weder *dasselbe* z_1 noch *dasselbe* z_2 mehr als einmal vorkommen, so lange man für z_1 Zahlen nimmt, die nicht schon z_2 berührten.

Geschieht *dies,* so ist das zugehörige z_2 wieder das z_1, welches $z_1 z_2 = \mathfrak{G}p + \varrho$ gab; so dafs also, wenn man z_1 *alle* die Zahlen (5.) durchlaufen läfst, jedes Product *zweimal* vorkommt und folglich die *Anzahl* der Producte $\frac{1}{2}(p-1)$ ist; indem hier in (5.) $p-1$ Zahlen z vorhanden sind. In diesen $\frac{1}{2}(p-1)$ Producten kommt aber dann kein z aus (5.) zweimal vor, während zugleich die z (5.) *alle* vorkommen.

Dieses zusammen ist was (III.) behauptet.

L. Anm. Der gegenwärtige Lehrsatz beruht im wesentlichen auf den Satz (§. 34.).

§. 48.

Lehrsatz.

Für jede ungerade Stammzahl* p > 1 *ist das Product

$$1. \quad 1.2.3.4....(p-1) = \mathfrak{G}p - 1.$$

Dieser Satz heifst nach seinem Erfinder der Wilsonsche Lehrsatz.

Beispiel.

$$2\left\{\begin{array}{l}\text{Für } p=3 \text{ giebt (1.) } 1.2=2=1.3-1;\\ - \quad p=5 \;-\;-\;-\; 1.2.3.4=24=5.5-1;\\ - \quad p=7 \;-\;-\;-\; 1.2.3.4.5.6=720=103.7-1;\\ - \quad p=11 \;-\;-\;-\; 1.2.3.4.5.6.7.8.9.10=3628800\\ \qquad\qquad\qquad\qquad =329891.11;\end{array}\right.$$

und so weiter; dem Lehrsatze gemäfs.

Beweis *A*. Aus den Zahlen

$$3. \quad z=2,\ 3,\ 4, \ldots\ p-2$$

geben *je zwei*, z_1 und z_2, gemäfs (§. 47. I.)

$$4. \quad z_1 z_2 = \mathfrak{S}p+1$$

und es sind nach (§. 47. I.) $\frac{1}{2}(p-3)$ solcher Producte vorhanden, in welchen dann z_1 und z_2 *alle* die Zahlen (3.) durchlaufen, ohne dafs irgend eine mehr als einmal vorkäme.

B. Daraus folgt, dafs das Product aller dieser $\frac{1}{2}(p-3)$ Producte (4.) das Product *aller* der Zahlen (3.) ist; und da nun *jedes* derselben $=\mathfrak{S}p+1$ ist, so ist

$$5. \quad 2.3.4.5 \ldots (p-2) = \mathfrak{S}p+1.$$

C. Multiplicirt man (5.) noch mit

$$6. \quad 1.(p-1) = \mathfrak{S}p-1,$$

so ergiebt sich

$$7. \quad 1.2.3.4 \ldots (p-1) = \mathfrak{S}p-1;$$

welches der Lehrsatz ist.

Weiter unten werden sich noch andere Beweise dieses Satzes finden.

§. 49.

Lehrsatz.

I. ***Es sei*** p ***eine Stammzahl*** >2, ***und*** r ***bezeichne die positiven oder negativen Quadratreste,*** ϱ ***die positiven oder negativen Nichtquadratreste zu*** p, ***so ist***

$$1. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1 \quad \text{und}$$

$$2. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1,$$

für alle r ***und*** ϱ, ***und*** (1.) ***nur für die*** r, (2.) ***nur für die*** ϱ. ***Alle möglichen, nicht mit*** p ***aufgehenden Zahlen*** r ***also, für welche die Gleichung*** (1.) ***Statt findet, sind Quadratreste zu der Stammzahl*** p; ***alle möglichen, nicht mit*** p ***aufgehenden Zahlen*** ϱ, ***für welche die Gleichung*** (2.)

Statt findet, sind Nichtquadratreste zu der Stammzahl p. *Die Anzahl der Quadratreste* r, *so wie der Nichtquadratreste* $\varrho > 0$ *und* $< p$ *ist* $\frac{1}{2}(p-1)$.

II. *Es seien* p *und* q *zwei Stammzahlen von der Form* $4n+1$ *oder* $4n-1$, *so ist,*

3. *wenn* p *zu* q, *zugleich* q *zu* p *positiver Quadratrest oder positiver Nichtquadratrest in allen Fällen wo* p *und* q *nicht beide von der Form* $4n-1$ *sind.*

4. *Ist* p *zu* q *positiver Quadratrest, so ist zugleich* q *zu* p *positiver Nichtquadratrest, und umgekehrt, in allen Fällen, wo* p *und* q *beide von der Form* $4n-1$ *sind.*

Dieses ist das Reciprocitätsgesetz in Beziehung auf Quadratreste und Nichtquadratreste.

Beispiele zu (I.). *a.* Es sei aus (§. 45. 13.)

5. $p=13$, $r=3$ und $\varrho=7$,

so ist $3^{\frac{1}{2}(p-1)}=3^6=27^2=(\mathfrak{S}p+1)^2=\mathfrak{S}p+1$, gemäfs (1.); und $7^6=49^3=(\mathfrak{S}p+10)^3=\mathfrak{S}p+1000=\mathfrak{S}p-1$; gemäfs (2.).

b. Es sei aus (§. 45. 13.)

6. $p=23$, $r=12$ und $\varrho=10$,

so ist für (1.) $r^2=144=\mathfrak{S}p+6$, $r^4=\mathfrak{S}p+36=\mathfrak{S}p+13$, $r^8=\mathfrak{S}p+169=\mathfrak{S}p+8$, $r^{10}=(\mathfrak{S}p+8)(\mathfrak{S}p+6)=\mathfrak{S}p+2$, $r^{11}=r^{\frac{1}{2}(p-1)}=(\mathfrak{S}p+2)12=\mathfrak{S}p+1$; gemäfs (1.).

Für (2.) ist $\varrho^2=100=\mathfrak{S}p+8$, $\varrho^4=\mathfrak{S}p-5$, $\varrho^8=\mathfrak{S}p+2$, $\varrho^{10}=(\mathfrak{S}p+2)(\mathfrak{S}p+8)=\mathfrak{S}p+16$, $\varrho^{11}=(\mathfrak{S}p+16).10=\mathfrak{S}p-1$; wie gehörig.

Beispiele zu (II.). *c.* Die Stammzahlen $p=13$ und $q=29$ sind beide von der Form $4n+1$. Einer der *Quadratreste* von p ist (§. 45. 13.) $2p+3=29=q$; also ist q *Quadratrest* zu p, und $p=13$ selbst ist Quadratrest zu $q=29$; gemäfs (3.).

d. $p=5$ und $q=13$ sind beide von der Form $4n+1$. Einer der *Nichtquadratreste* zu 5 ist (§. 45. 13.) $2.5+3=13$, also $=q$, und zugleich ist $p=5$ selbst *Nichtquadratrest* zu $q=13$; gemäfs (3.).

e. $p=23$, von der Form $4n-1$, ist *Quadratrest* zu $q=29=4n+1$ (§. 45. 13.); auch $q=29$ ist *Quadratrest* zu $p=23$, nemlich $=1.p+6$; gemäfs (3.).

f. $p = 11$, von der Form $4n - 1$, ist ***Nichtquadratrest*** zu $q = 29$ (§. 45. 13.); und auch $q = 29$ ist ***Nichtquadratrest*** zu $p = 11$, nemlich $= 2p + 7$; gemäſs (3.).

g. $p = 13$, von der Form $4n + 1$, ist ***Quadratrest*** zu $q = 23 = 4n - 1$; und auch $q = 23$ ist ***Quadratrest*** zu $p = 13$ (§. 45. 13.), nemlich $= 1.p + 4$; gemäſs (3.).

h. $p = 17 = 4n + 1$ ist ***Nichtquadratrest*** zu $q = 31 = 4n - 1$; und auch $q = 31$ ist ***Nichtquadratrest*** zu $p = 17$, nemlich $= 1.p + 14$ (§. 45. 13.), gemäſs (3.).

i. $p = 7 = 4n - 1$ ist ***Quadratrest*** zu $q = 31 = 4n - 1$. Dagegen ist $q = 31$ ***Nichtquadratrest*** zu $p = 7$, nemlich $= 4.p + 3$ (§. 45. 13.); gemäſs (4.).

k. $p = 11 = 4n - 1$ ist ***Nichtquadratrest*** zu $q = 31 = 4n - 1$. Dagegen ist $q = 31$ ***Quadratrest*** zu $p = 11$, nemlich $= 2p + 9$ (§. 45. 13.); gemäſs (4.).

Erster Beweis von (I.). ***A.*** Nach dem Fermatschen Lehrsatze (40.) ist

$$7. \quad z^{p-1} - 1 = \mathfrak{G}p,$$

und daraus folgt, weil $p - 1$ ***immer gerade*** ist,

$$8. \quad (z^{\frac{1}{2}(p-1)} - 1)(z^{\frac{1}{2}(p-1)} + 1) = \mathfrak{G}p,$$

also muſs entweder $z^{\frac{1}{2}(p-1)} - 1$ oder $z^{\frac{1}{2}(p-1)} + 1$ mit p ***aufgehen,*** das heiſst es muſs

$$9. \quad \text{entweder} \quad z^{\frac{1}{2}(p-1)} - 1 = \mathfrak{G}p$$

$$10. \quad \text{oder} \quad z^{\frac{1}{2}(p-1)} + 1 = \mathfrak{G}p$$

sein.

B. Die Gleichung (7.) hat $p - 1$ ***Wurzeln,*** denn sie findet nach (§. 40.) für ***alle*** die $p - 1$ Werthe $1, 2, 3, 4, \ldots p - 1$ von z Statt. Also muſs auch (8.), und folglich müssen (9. und 10.), diese letztern ***zusammen,*** für $p - 1$ verschiedene Werthe von z Statt finden.

C. Ein- und derselbe Werth von z kann nicht (9.) und (10.) ***zugleich*** erfüllen, denn sonst wäre, (9.) von (10.) abgezogen,

$$11. \quad z^{\frac{1}{2}(p-1)} + 1 - (z^{\frac{1}{2}(p-1)} - 1) = 2 = \mathfrak{G}p,$$

und 2 geht ***nicht*** mit p auf. Alle Wurzeln von (9.) müssen also von denen von (10.) ***verschieden*** sein.

D. Nun kann nach (§. 44.) (9.), und eben so (10.), ***nicht mehr*** als $\frac{1}{2}(p-1)$ Wurzeln haben. Deshalb kann z. B. (9.) auch ***nicht weniger*** als $\frac{1}{2}(p-1)$ Wurzeln haben, denn wäre das, so müſste, weil (9. und 10.) ***zusammen*** $p - 1$ Wurzeln haben müssen (***B.***), (10.) ***mehr*** als $\frac{1}{2}(p-1)$ Wurzeln

haben, was nach (§. 44.) nicht sein kann. Folglich mufs (9.), da es ***nicht mehr*** und ***nicht weniger*** als $\frac{1}{2}(p-1)$ Wurzeln haben kann, nothwendig gerade $\frac{1}{2}(p-1)$ verschiedene Wurzeln haben, und folglich (10.) die übrigen $\frac{1}{2}(p-1)$ Wurzeln, die nach (*C.*) alle von den Wurzeln von (9.) verschieden sind. Die Gleichungen (9. und 10.) theilen sich also zu zwei ***gleichen*** Theilen in die $p-1$ Wurzeln $1, 2, 3, 4, \ldots\, p-1$ von (7.).

E. Setzt man nun für alle Werthe von z,

$$12. \quad z^2 = \mathfrak{G}p + r,$$

wo $r > 0$ und $< p$, so bezeichnet r alle ***Quadratreste.*** Nimmt man von (12.) die $\frac{1}{2}(p-1)$ten Potenz, so ergiebt sich

$$13. \quad z^{2\cdot\frac{1}{2}(p-1)} = z^{p-1} = (\mathfrak{G}p + r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + r^{\frac{1}{2}(p-1)} \text{ (§. 11. 20.)},$$

und da nach dem Fermatschen Lehrsatz (§. 40.), für ***alle*** Werthe von z, $z^{p-1} = \mathfrak{G}p + 1$ ist,

$$\mathfrak{G}p + 1 = \mathfrak{G}p + r^{\frac{1}{2}(p-1)} \text{ oder}$$

$$14. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \text{ oder } r^{\frac{1}{2}(p-1)} - 1 = \mathfrak{G}p.$$

F. Es sind aber die Quadratreste r, da sie > 0 und $< p$ sind, ebensowohl Werthe von z: also ist (14.) nichts anders als (9.); und da nun (9.) zufolge (***D.***) nothwendig für $\frac{1}{2}(p-1)$ Werthe von z (für nicht mehr und nicht weniger) Statt findet, so hat in (14.) r nothwendig $\frac{1}{2}(p-1)$ verschiedene Werthe. Folglich giebt es nothwendig $\frac{1}{2}(p-1)$ verschiedene ***Quadratreste*** r, nicht mehr und nicht weniger, unter den Werthen von $z > 0$ und $< p$, und für jeden derselben findet die Gleichung (14.) Statt, welche diejenige (1.) des Lehrsatzes ist.

G. Da r in (14.) oder (1.) ***nur*** $\frac{1}{2}(p-1)$ Werthe haben kann, so bleiben $\frac{1}{2}(p-1)$ Werthe von z übrig, welche nach (*C.*) diejenigen sind, die der Gleichung (10.) genugthun. Da sie keine Quadratreste sind, für welche ***nur*** die Gleichung (9.) gilt, so sind sie die ***Nichtquadratreste*** ϱ, und folglich giebt es auch $\frac{1}{2}(p-1)$ ***Nichtquadratreste,*** und für jeden derselben findet nach (10.) die Gleichung

$$15. \quad \varrho^{\frac{1}{2}(p-1)} + 1 = \mathfrak{G}p$$

Statt, welche nichts anderes als die Gleichung (2.) des Lehrsatzes ist.

H. Übrigens kann r und ϱ auch $> p$ sein, z. B. r_1 und ϱ_1, wenn nur

$$16. \quad r_1 = \mathfrak{G}p + r \text{ und}$$

$$17. \quad \varrho_1 = \mathfrak{G}p + \varrho$$

ist. Dieses zusammen behauptet (I.).

Zweiter Beweis von I. *I.* Aus den Zahlen

$$18. \quad z = 1, 2, 3, 4, \ldots p-1$$

geben je *zwei*, z_1 und z_2, gemäfs (§. 47. III.),

$$19. \quad z_1 z_2 = \mathfrak{S}p + \varrho,$$

wo ϱ ein beliebiger *Nichtquadratrest* zu p ist, und es sind nach (§. 47. III.) $\frac{1}{2}(p-1)$ solcher Producte vorhanden, in welchen dann z_1 und z_2 *alle* die Zahlen (13.) durchlaufen, ohne dafs irgend eine mehr als einmal vorkäme.

K. Daraus folgt, dafs das Product aller der $\frac{1}{2}(p-1)$ Producte (19.) das Product *aller* der Zahlen (18.) ist; und da nun *jedes* der $\frac{1}{2}(p-1)$ Producte (19.) $z_1 z_2 = \mathfrak{S}p + \varrho$ giebt, so ist

$$20. \quad 1.2.3.4 \ldots (p-1) = (\mathfrak{S}p + \varrho)^{\frac{1}{2}(p-1)} = \mathfrak{S}p + \varrho^{\frac{1}{2}(p-1)}.$$

L. Aber gemäfs (§. 48.) ist

$$21. \quad 1.2.3.4 \ldots (p-1) = \mathfrak{S}p - 1,$$

also ist, zufolge (20. und 21.), $\mathfrak{S}p + \varrho^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1$ oder

$$22. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1;$$

gemäfs (2.).

M. Für *jede* Zahl $< p$, also auch für jeden *Quadratrest* r zu p, ist nach dem Fermatschen Satz (§. 40.)

$$23. \quad r^{p-1} = \mathfrak{S}p + 1.$$

Daraus folgt

$$24. \quad r^{p-1} - 1 \quad \text{oder} \quad (r^{\frac{1}{2}(p-1)} + 1)(r^{\frac{1}{2}(p-1)} - 1) = \mathfrak{S}p,$$

also mufs entweder $r^{\frac{1}{2}(p-1)} + 1$ oder $r^{\frac{1}{2}(p-1)} - 1$ mit p *aufgehen*, das heifst, es mufs

$$25. \quad \text{entweder } r^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1,$$

$$26. \quad \text{oder } r^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1$$

sein. Das erste kann nicht sein, denn sonst müfste nach (22.) r nicht ein Quadratrest, sondern ein *Nichtquadratrest* ϱ sein. Also kann nur

$$27. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1$$

sein; gemäfs (1.).

Beweis von (II.). *N.* Nach dem Reciprocitätsgesetze (§. 42.) ist *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q + 1$, oder *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q - 1$, wenn p und q *nicht beide* von der Form $4n-1$ sind. Also ist in diesem Fall, gemäfs (1. und 2.), entweder q einer der *Quadratreste* zu p und *zugleich* p einer der *Quadratreste* zu q, oder q einer der *Nichtquadratreste* zu p und *zugleich* p einer der *Nichtquadratreste* zu q; gemäfs (3.).

O. Sodann ist nach dem Reciprocitätsgesetze (§. 42.) ***zugleich*** $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q-1$, oder ***zugleich*** $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{S}q+1$, wenn p und q ***beide*** von der Form $4n-1$ sind. Also ist in diesem Falle gemäfs (1. und 2.) entweder q einer der ***Quadratreste*** zu p, und ***zugleich*** p einer der *Nichtquadratreste* zu q, oder q einer der Nichtquadratreste zu p, und ***zugleich*** p einer der ***Quadratreste*** zu q, gemäfs (4.).

Erste Anm. ***P.*** Der *erste* Beweis von (I.), welcher (II.) unmittelbar begründet, beruht insbesondere auf dem Fermatschen Satze (§. 40.) und auf dem Satze (§. 44.) von der Anzahl der Wurzeln von Zahlengleichungen; der *zweite* Beweis von (I.) beruht auf dem Wilsonschen Satze (§. 48.) und auf dem Satze (§. 47.) von den ***zusammengehörigen*** Zahlen. Der zweite Beweis bedarf also weniger Vordersätze als der erste. Eigenthümlich ist in dem ersten Beweise die Folgerung in (***D.***), dafs, da von den ***beiden*** Gleichungen (9. und 10.) keine ***mehr als*** $\frac{1}{2}(p-1)$ Wurzeln haben kann und beide zusammen nothwendig $p-1$ Wurzeln haben, jede $\frac{1}{2}(p-1)$ Wurzeln haben ***mufs.***

Zweite Anm. ***Q.*** Wegen der Beziehung (II.) des Reciprocitäts- oder Gegenseitigkeits-Gesetzes auf die ***Quadratreste*** und ***Nichtquadratreste*** könnte man dasselbe ***Gegenquadratrestgesetz*** nennen. Diese Benennung würde ***deutlicher bezeichnen*** was gemeint ist, als das Wort ***Gegenseitigkeitsgesetz.*** Da es indessen etwas länger ist und das Gegenseitigkeitsgesetz auch in seiner ursprünglichen Form (§. 42.) vorkommt, so wollen wir von „***Gegenquadratrestgesetz***" nicht Gebrauch machen.

Ferner wäre ***Gegenheitsgesetz*** kürzer und einfacher als Gegenseitigkeitsgesetz, und ***Gegenheit*** würde nach dem Vorbilde von ***Gleichheit, Allgemeinheit, Besonderheit, Gewifsheit*** u. s. w. grammatisch nicht unrichtig sein. Da indessen wieder das Wort Gegenheit noch vielleicht ***zu neu*** ist, so wollen wir die kürzere Benennung blofs anheimstellen, und uns nur begnügen, das verstümmelte fremde Wort Reciprocität zu vermeiden, mithin den Satz (§. 42.) oder (§. 49. II.) ***Gegenseitigkeitsgesetz*** nennen.

§. 50.

Lehrsatz.

I. ***Für alle Stammzahlen*** p = 4n+1 ***sind die zeichenfreien Werthe der positiven und der negativen echten Quadratreste dieselben. Gleiches gilt von den Nichtquadratresten.***

II. *Für alle Stammzahlen* $p = 4n - 1$ *sind die positiven echten Quadratreste die zeichenfreien Werthe der negativen echten Nichtquadratreste, und die positiven echten Nichtquadratreste die zeichenfreien Werthe der negativen echten Quadratreste.*

Beispiele. Was (I.) behauptet, zeigt sich in (§. 45. 13.) an den Stammzahlen 5, 13, 17 und 29, die von der Form $4n + 1$ sind.

Was (II.) behauptet, zeigt sich in (§. 45. 13.) an den Stammzahlen 3, 7, 11, 19, 23 und 31, die von der Form $4n - 1$ sind.

Beweis *A.* Für *alle*, und folglich auch für alle *echten positiven Quadratreste* r findet nach (§. 49. 1.) die Gleichung

$$1. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1,$$

und für *alle*, also auch für alle echten positiven *Nichtquadratreste* nach (§. 49. 2.), die Gleichung

$$2. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1$$

Statt.

B. Alle echten *negativen* Quadratreste werden durch $r - p$ ausgedrückt, also ihre *zeichenfreien* Werthe durch $p - r$; denn $p - r$ ist > 0 und $< p$.

Je nachdem also die durch $p - r$ ausgedrückten Zahlen

$$3. \quad (p - r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1, \text{ oder}$$

$$4. \quad (p - r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1$$

geben, werden sie zufolge (§. 49. 1. u. 2.) *Quadratreste* oder *Nichtquadratreste* zu p sein.

C. Da

$$5. \quad (p - r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + (-r)^{\frac{1}{2}(p-1)}$$

ist, so erfordert nach (3.) das Erste, dafs

$$6. \quad \mathfrak{G}p + (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1, \text{ also } (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1,$$

das Andere nach (4.), dafs

$$7. \quad \mathfrak{G}p + (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1, \text{ also } (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1$$

sei.

D. Ist nun $p = 4n + 1$, so ist $\frac{1}{2}(p - 1) = 2n$ und folglich $\frac{1}{2}(p - 1)$ eine *gerade* Zahl. Also ist alsdann $(-r)^{\frac{1}{2}(p-1)} = (+r)^{\frac{1}{2}(p-1)}$, und da nach (1.) $(+r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1$ ist, so wird für $p = 4n + 1$ die Gleichung (6.) erfüllt. Also sind für $p = 4n + 1$ die Zahlen $p - r$ echte positive *Quadratreste,* und folglich sind die echten *negativen* Quadratreste $r - p$ ihrem *zeichenfreien* Werthe nach den echten positiven *Quadratresten* r *gleich.*

Und da die echten positiven *Nichtquadratreste* ϱ übrig bleiben, wenn man die echten positiven *Quadratreste* r aus den Zahlen $1, 2, 3, 4, \ldots p-1$ wegnimmt; desgleichen die echten negativen *Nichtquadratreste* $-\varrho$, wenn man die echten negativen *Quadratreste* aus $-(1, 2, 3, 4, \ldots p-1)$ wegläfst, so sind auch nothwendig die echten ***negativen Nichtquadratreste*** ihrem ***zeichenfreien*** Werthe nach den echten ***positiven Nichtquadratresten gleich.***

Dieses ist was (I.) behauptet.

E. Ist dagegen $p = 4n-1$, so ist $\frac{1}{2}(p-1) = 2n-1$, und folglich $\frac{1}{2}(p-1)$ eine ***ungerade*** Zahl. Also ist alsdann $(-r)^{\frac{1}{2}(p-1)} = -(+r)^{\frac{1}{2}(p-1)}$, und da nach (1.) $(+r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, also $-(+r)^{\frac{1}{2}(p-1)} = -\mathfrak{G}p-1 = \mathfrak{G}p-1$ ist, so wird für $p = 4n-1$ die Gleichung (7.) erfüllt. Also sind für $p = 4n-1$ die Zahlen $p-r$ echte positive *Nichtquadratreste,* und folglich die echten ***negativen*** Quadratreste $r-p$ ihrem ***zeichenfreien*** Werthe $p-r$ nach den echten ***positiven Nichtquadratresten*** ϱ gleich.

Und da nun die echten negativen *Nichtquadratreste* $-\varrho$ durch $\varrho - p$ ausgedrückt werden, so sind sie, weil $p-r=\varrho$ war, gleich $p-r-p = -r$; folglich ist der ***zeichenfreie*** Werth r der ***negativen*** echten ***Quadratreste*** $-r$ der der ***negativen*** echten ***Nichtquadratreste*** ϱ.

Dieses ist was (II.) behauptet.

F. Anm. Der Satz beruht insbesondere auf (§. 49.).

§. 51.

Lehrsatz.

I. ***Für jede Stammzahl*** p $= 4n+1$ ***ist die Summe der zeichenfreien Werthe je zweier positiver oder je zweier negativer echter Quadratreste, so wie die Summe der zeichenfreien Werthe je zweier positiver oder je zweier negativer echter Nichtquadratreste, gleich*** p.

II. ***Für jede Stammzahl*** p $= 4$n-1 ***ist die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten Quadratrests, so wie die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten Nichtquadratrests gleich*** p.

Beispiel. In (§. 45. 13.) sieht man was (I.) behauptet an den Stammzahlen $p = 5, 13, 17$ und 29, die von der Form $4n+1$ sind, und was (II.) behauptet an den Stammzahlen 3, 7, 11, 19, 23 und 31, die von der Form $4n-1$ sind.

Beweis *A*. Je nachdem $p-r$ ein echter positiver *Quadratrest,* oder ein echter positiver *Nichtquadratrest* ist, wird die Summe zweier echter positiver, oder die Summe eines echten positiven und eines echten negativen *Nichtquadratrests* gleich p sein.

B. Soll nun $p-r$ ein echter positiver *Quadratrest* sein, so mufs es nach (§. 49. 1.) die Gleichung

$$1.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$$

erfüllen. Soll $p-r$ ein echter positiver *Nichtquadratrest* sein, so mufs es nach (§. 49. 2.) der Gleichung

$$2.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1$$

genugthun.

C. *Ersteres* geschieht, wenn $p=4n+1$ ist; denn die Gleichung (1.) ist so viel als $\mathfrak{S}p+(-r)^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ oder

$$3.\quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1,$$

und da hier $\frac{1}{2}(p-1)=2n=$ einer *geraden* Zahl ist, so ist $(-r)^{\frac{1}{2}(p-1)}=(+r)^{\frac{1}{2}(p-1)}$, also in (3.)

$$4.\quad +r^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1,$$

und folglich auch nach (1.)

$$5.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1.$$

Mithin ist $p-r$ wirklich ein echter positiver *Quadratrest.* Also ist zunächst

a. Die *Summe* je zweier echter positiver Quadratreste $=p$.

b. Die *zeichenfreien* Werthe der echten negativen *Quadratreste* sind in dem Falle $p=4n+1$ nach (§. 50. I.) den echten positiven *Quadratresten gleich.* Also ist auch die Summe der *zeichenfreien* Werthe zweier echter negativer Quadratreste $=p$.

c. Die positiven echten *Nichtquadratreste* ϱ bleiben aus den Zahlen $1, 2, 3, 4, \ldots\ldots p-1$ übrig, wenn man davon die echten positiven Quadratreste r wegläfst. Also ist *kein* ϱ einem r gleich. Mithin ist auch kein $p-\varrho$ einem $p-r$ gleich, und mithin, da nach (*a*.) *jedes* $p-r$ einem r gleich ist, auch kein $p-\varrho$ einem r. Aber $p-\varrho$ ist, eben wie ϱ, nothwendig unter den Zahlen $1, 2, 3, 4, \ldots\ldots p-1$ anzutreffen, weil $p-\varrho>0$ und $<p$ ist: also ist nothwendig jedes $p-\varrho$ einem ϱ *gleich.* Das heifst: auch die Summe je zweier echter positiver *Nichtquadratreste* ist $=p$.

d. Endlich sind nach (§. 50. I.) die zeichenfreien Werthe der negativen echten *Nichtquadratreste* den positiven echten *Nichtquadratresten gleich.*

Also ist auch die Summe der zeichenfreien Werthe je zweier echter negativer *Nichtquadratreste* $= p$.

Dieses zusammen ist, was (I.) behauptet.

D. Die zweite Gleichung (2.) in (*B.*) wird erfüllt, wenn $p = 4n - 1$ ist; denn die Gleichung (2.) ist so viel als $\mathfrak{G} p + (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G} p - 1$ oder

$$6. \quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G} p - 1,$$

und da hier $\frac{1}{2}(p-1) = 2n-1 =$ einer *ungeraden* Zahl ist, so ist $(-r)^{\frac{1}{2}(p-1)} = -(+r)^{\frac{1}{2}(p-1)}$, also ist in (6.)

$$7. \quad -(+r)^{\frac{1}{2}(p-1)} = \mathfrak{G} p - 1 \text{ oder}$$

$$8. \quad (+r)^{\frac{1}{2}(p-1)} = -\mathfrak{G} p + 1 = \mathfrak{G} p + 1.$$

Dieses ist der Gleichung (§. 49. 1.) für alle echten positiven *Quadratreste* $+r$ gemäfs. Also erfüllt in dem gegenwärtigen Falle $p = 4n - 1$, $p - r$ die Gleichung (2.) wirklich, und folglich ist für $p = 4n - 1$ die Summe der zeichenfreien Werthe je eines positiven Quadratrests und eines positiven echten *Nichtquadratrests* $= p$.

Aber die positiven echten *Nichtquadratreste* sind nach (§. 50. II.) den zeichenfreien Werthen der negativen echten *Quadratreste gleich.* Also ist

a. Die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten *Quadratrestes* $= p$.

d. Ferner sind nach (§. 50. II.) die echten positiven *Quadratreste* den zeichenfreien Werthen nach den negativen echten *Nichtquadratresten* gleich. Also ist auch die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten *Nichtquadratrestes* $= p$.

Dieses zusammen ist was (II.) behauptet.

Anm. *E.* Der Beweis beruht auf (§. 49. und 50.). Eigenthümlich ist der Schlufs in (*C. c.*).

§. 52.

Lehrsatz.

I. ***Das Product einer beliebigen Anzahl von Quadratresten zu einer und derselben Stammzahl* p *ist ein Quadratrest zu* p.**

II. ***Das Product einer beliebigen geraden Anzahl von Nichtquadratresten, eben so, ist ein Quadratrest.***

III. ***Das Product einer beliebigen ungeraden Anzahl von beliebigen Nichtquadratresten, eben so, ist ein Nichtquadratrest.***

IV. ***Das Product eines Quadratrestes und eines Nichtquadratrestes ist ein Nichtquadratrest.***

Beispiele. 1. Zu I. $+8$, -10 und 4 sind *Quadratreste* zu $p=7$ (§. 45. 13.), und ihr Product ist $-320=-46.7+2$, also ebenfalls ein *Quadratrest* zu p.

2. Zu II. 18, -5, 7 und 15 sind *Nichtquadratreste* zu $p=13$ (§. 45. 13.), und ihr Product ist $-9450=-727.13+1$, also ein *Quadratrest* zu p.

3. Zu III. $+32$, -32 und 40 sind *Nichtquadratreste* zu $p=29$ (§. 45. 13.), und ihr Product $32^2.40$ ist $=40960=1412.29+12$, also ebenfalls ein *Nichtquadratrest* zu p.

4. Zu IV. -11 ist ein *Quadratrest* und $+33$ ein *Nichtquadratrest* zu $p=23$ (§. 45. 13.), und ihr Product -363 ist $=-16.23+5$, also ein *Nichtquadratrest* zu p.

Beweis. Für jeden *beliebigen Quadratrest* r ist nach (§. 49. 1.)

$$1.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1$$

und für jeden *beliebigen Nichtquadratrest* ϱ nach (§. 49. 2.)

$$2.\quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1.$$

Multiplicirt man also eine *beliebige Anzahl* von r in einander, so ist das Product gemäfs (1.) immer $=\mathfrak{S}p+1$, und folglich ebenfalls ein *Quadratrest*; gemäfs (I.).

Multiplicirt man eine *beliebige gerade Anzahl* von *Nichtquadratresten* in einander, so ist das Product gemäfs (2.) immer $=\mathfrak{S}p+1$, also ebenfalls ein *Quadratrest*; gemäfs (II.).

Multiplicirt man dagegen eine *beliebige ungerade* Anzahl von *Nichtquadratresten* in einander, so ist das Product gemäfs (2.) immer $=\mathfrak{S}p-1$, und folglich ein *Nichtquadratrest*; gemäfs (III.).

Multiplicirt man (1.) in (2.), so ist das Product $=\mathfrak{S}p-1$, und folglich ein *Nichtquadratrest*; gemäfs (IV.).

Anm. Der Beweis geht unmittelbar aus (§. 49.) hervor.

§. 53.

Lehrsatz.

I. $+1$ ist *Quadratrest* zu allen Stammzahlen ohne Ausnahme.

II. -1 ist *Quadratrest* zu allen Stammzahlen $p=4n+1$
und *Nichtquadratrest* zu allen Stammzahlen $p=4n-1$.

III. $+2$ ist *Quadratrest* zu allen Stammzahlen $p=8n+1$ und $p=8n-1$
und *Nichtquadratrest* zu allen Stammzahlen $p=8n+3$ und $p=8n-3$.

IV. -2 ist *Quadratrest* zu allen Stammzahlen $p=8n+1$ und $p=8n+3$ und *Nichtquadratrest* zu allen Stammzahlen $p=8n-1$ und $p=8n-3$.

Beispiele. *a.* In allen den Beispielen (§. 45. 13.) ist, wie sich zeigt, $+1$ einer der *Quadratreste.*

b. -1 ist unter den *Quadratresten* zu $p=5$, 13, 17 und 29, und diese p sind von der Form $4n+1$.

-1 ist unter den *Nichtquadratresten* zu $p=3$, 7, 11, 19, 23 und 31, und diese Stammzahlen sind von der Form $4n-1$.

c. $+2$ ist unter den *Quadratresten* zu $p=17=8n+1$ und $p=7, 23$ und $31=8n-1$.

$+2$ ist unter den *Nichtquadratresten* zu $p=3$, 11 und $19=8n+3$ und $p=5$, 13 und $29=8n-3$.

d. -2 ist unter den *Quadratresten* zu $p=17=8n+1$ und $p=3, 11$ und $19=8n+3$.

-2 ist unter den *Nichtquadratresten* zu $p=7$ und $23=8n-1$ und $p=5, 13$ und $29=8n-3$.

Beweis von I. ***A.*** Für alle Zahlen r, welche Quadratreste zu der Stammzahl p sind, ist nach (§. 49. 1.)

$$1.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1.$$

Dieser Gleichung wird durch $r=+1$ genuggethan; was auch p sein mag. Also ist $+1$ *Quadratrest* zu *jeder* Stammzahl p.

Beweis von II. ***B.*** Der Gleichung (1.) wird durch $r=-1$ nur dann genuggethan, wenn $\frac{1}{2}(p-1)$ *gerade* ist. Dieses ist der Fall für $p=4n+1$, welches $\frac{1}{2}(p-1)=2n$ giebt; nicht für $p=4n-1$; denn dieses giebt $\frac{1}{2}(p-1)=2n-1$, also eine *ungerade* Zahl. Mithin ist -1 *Quadratrest* zu allen Stammzahlen $p=4n+1$.

C. Sodann ist für alle Zahlen ϱ, welche *Nichtquadratreste* zu der Stammzahl p sind, nach (§. 49. 2.),

$$2.\quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1.$$

Dieser Gleichung wird durch $\varrho=-1$ genuggethan, wenn $\frac{1}{2}(p-1)$ *ungerade* ist. Dieses ist, wie so eben in (***B.***) bemerkt, der Fall, wenn $p=4n-1$ ist. Also ist -1 *Nichtquadratrest* zu allen Stammzahlen $p=4n-1$.

Beweis von III. ***D.*** Man multiplicire alle die Zahlen 1, 2, 3, 4, ... $\frac{1}{2}(p-1)$ mit 2. Dieses giebt

3. Für $p=8n+1$, 2.1, 2.2, 2.3, 2.4, ... $2.2n$ und
$2(2n+1)$, $2(2n+2)$, $2(2n+3)$, ... $2.4n$;

4. Für $p=8n-1$, 2.1, 2.2, 2.3, 2.4, ... $2(2n-1)$ und
$2.2n$, $2(2n+1)$, $2(2n+2)$, ... $2(4n-1)$;

5. Für $p=8n+3$, 2.1, 2.2, 2.3, 2.4, ... $2.2n$ und
$2(2n+1)$, $2(2n+2)$, $2(2n+3)$, ... $2(4n+1)$;

6. Für $p=8n-3$, 2.1, 2.2, 2.3, 2.4, ... $2(2n-1)$ und
$2.2n$, $2(2n+1)$, $2(2n+2)$, ... $2(4n-2)$.

In diesen vier verschiedenen Productenreihen sind alle die, welche ***vor*** dem Worte ***und*** stehen, $<\frac{1}{2}p$, denn die *gröfsten* derselben sind $2.2n=4n<\frac{1}{2}(8n+1)$, $2(2n-2)=4n-1<\frac{1}{2}(8n-1)$; $2.2n=4n<\frac{1}{2}(8n+3)$ und $2(2n-1)=4n-2<\frac{1}{2}(8n-3)$: alle Producte, die nach dem Worte ***und*** stehen, sind $>\frac{1}{2}p$ oder $<p$; denn die ***kleinsten*** derselben sind $2(2n+1)=4n+2>\frac{1}{2}(8n+1)$; $2.2n=4n>\frac{1}{2}(8n-1)$; $2(2n+1)=4n+2>\frac{1}{2}(8n+3)$ und $2.2n=4n>\frac{1}{2}(8n-3)$; die gröfsten dagegen $2.4n=8n<8n+1$; $2(4n-1)=8n-2<8n-1$; $2(4n+1)=8n+2<8n+3$ und $2(4n-2)=8n-4<8n-3$.

E. Die ***Anzahl*** der Producte in (3. 4. 5. 6.), die $>\frac{1}{2}p$ sind, und welche durch $\varkappa$ bezeichnet werden mag, ist

7. In (3.), für $p=8n+1$, $\varkappa=2n$, also *gerade;*

8. In (4.), für $p=8n-1$, $\varkappa=2n$, also *gerade;*

9. In (5.), für $p=8n+3$, $\varkappa=2n+1$, also *ungerade;*

10. In (6.), für $p=8n-3$, $\varkappa=2n-1$, also *ungerade.*

F. Nun ist zufolge (§. 41. 3. und 4.), wenn man daselbst $x=2$ setzt,

11. $2^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$, wenn $\varkappa$ *gerade* und

12. $2^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$, wenn $\varkappa$ *ungerade* ist.

Also erfüllt $r=2$ die Gleichung (1.), wenn $\varkappa$ *gerade,* also $p=8n+1$ oder $p=8n-1$, und $\varrho=2$ die Gleichung (2.), wenn $\varkappa$ *ungerade,* also $p=8n+3$ oder $p=8n-3$ ist. Und folglich ist $+2$ *Quadratrest* zu $p=8n+1$ und $p=8n-1$, und *Nichtquadratrest* zu $p=8n+3$ und $p=8n-3$; gemäfs (III.).

Erster Beweis von IV. ***G.*** Es war $+1$ *Quadratrest* zu *allen* Stammzahlen ohne Ausnahme, also zu $p=8n+1$, $8n-1$, $8n+3$ und $8n-3$ (I.). Ferner war -1 *Quadratrest* zu $p=4n+1$ (II.), also zu den Stammzahlen $p=8n+1$ und $p=8n-3$, die von der Form $4n+1$ sind, wie sich zeigt, wenn man in $4n+1$ erst $2n$ und dann $2n-1$ statt n

setzt (was geschehen darf, indem $2n$ und $2n-1$ zusammen ebensowohl *alle* geraden und ungeraden Zahlen ausdrücken, wie n selbst), und was dann $4.2n+1=8n+1$ und $4(2n-1)+1=8n-3$ giebt. Und endlich war -1 *Nichtquadratrest* zu $p=4n-1$ (II.), also zu den Stammzahlen $p=8n-1$ und $p=8n+3$, die von der Form $4n-1$ sind, wie sich zeigt, wenn man in $4n-1$ erst $2n$ und dann $2n+1$ statt n setzt, was wie vorhin geschehen darf und was $4.2n-1=8n-1$ und $4(2n+1)-1=8n+3$ giebt.

H. Nimmt man dies mit dem was der Lehrsatz in (III.) für $+2$ aussagt zusammen, so ergiebt sich Folgendes:

13.

Zu	$p=8n+1$,	$8n-1$,	$8n+3$	und $8n-3$	
sind	$+1$	$+1$	$+1$	$+1$	*Quadratrest*
	-1	...	...	...	
	$+2$	$+2$	...	...	
und	...	-1	-1	...	*Nichtquadratrest.*
	...	...	$+2$	$+2$	

Nun erhält man in (13.) -2, wenn man

14. Für $p=8n+1$, den *Quadratrest* -1 mit dem *Quadratrest* $+2$,
- $p=8n-1$, den *Quadratrest* $+2$ mit dem *Nichtquadratrest* -1,
- $p=8n+3$, den *Nichtquadratrest* -1 mit dem *Nichtquadratrest* $+2$,
- $p=8n-3$, den *Quadratrest* -1 mit dem *Nichtquadratrest* $+2$

multiplicirt. Aber das Product zweier *Quadratreste* und zweier *Nichtquadratreste* ist nach (§. 52. I. und II.) ein *Quadratrest*, und das Product eines *Quadratrests* und eines *Nichtquadratrests* nach (§. 52. III.) ein *Nichtquadratrest:* also folgt aus (14.), dafs -2 *Quadratrest* zu $p=8n+1$ und $p=8n+3$ und *Nichtquadratrest* zu $p=8n-1$ und $p=8n-3$ ist; gemäfs (IV.).

Zweiter Beweis von IV. ***I.*** Man multiplicire (11. und 12.) mit $(-1)^{\frac{1}{2}(p-1)}$. Dieses giebt

15. $(-2)^{\frac{1}{2}(p-1)}=\mathfrak{S}p+(-1)^{\frac{1}{2}(p-1)}$, wenn z *gerade*, also $p=8n+1$ oder $p=8n-1$ ist (7. und 8.), und

16. $(-2)^{\frac{1}{2}(p-1)}=\mathfrak{S}p-(-1)^{\frac{1}{2}(p-1)}$, wenn z *ungerade*, also $p=8n+3$ oder $p=8n-3$ ist (9. und 10.).

Nun ist

$$17.\begin{cases} 1.\ \text{Für}\ p = 8n+1,\ \tfrac{1}{2}(p-1) = 4n,\ \text{also}\ \textit{gerade}; \\ 2.\ \ -\ \ p = 8n-1,\ \tfrac{1}{2}(p-1) = 4n-1,\ \textit{also ungerade}; \\ 3.\ \ -\ \ p = 8n+3,\ \tfrac{1}{2}(p-1) = 4n+1,\ \text{also}\ \textit{ungerade}; \\ 4.\ \ -\ \ p = 8n-3,\ \tfrac{1}{2}(p-1) = 4n-2,\ \text{also}\ \textit{gerade}; \end{cases}$$

folglich geben (15. und 16.)

$$18.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1 \quad \text{für} \quad p = 8n+1;$$
$$19.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1 \quad \text{für} \quad p = 8n-1;$$
$$20.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1 \quad \text{für} \quad p = 8n+3;$$
$$21.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1 \quad \text{für} \quad p = 8n-3.$$

Die Gleichungen (18. und 20.) erfüllen diejenigen (1.) für $r = -2$, also ist -2 *Quadratrest* zu $p = 8n+1$ und $8n+3$. Dagegen erfüllen die Gleichungen (19. und 21.) die Gleichung (2.) für $\varrho = -2$, also ist -2 *Nichtquadratrest* zu $p = 8n-1$ und $p = 8n-3$; gemäfs (IV.).

Anm. *1.* Die Beweise beruhen auf einer Verbindung der Sätze (§. 41. 49. und 52.).

§. 54.

Lehrsatz.

Wenn in den Zahlengleichungen (S. §. 43.)

$$1.\quad z^{\delta} = \mathfrak{S}p+r \quad \text{und}$$
$$2.\quad z^{\lambda} = \mathfrak{S}p+\varrho$$

p *eine Stammzahl ist,* r *und* $\varrho > 0$ *und* $<$ p *sind, und der Exponent* δ *in* p — 1, *der Exponent* λ *in* δ *und also ebenfalls in* p — 1 *aufgeht, so dafs z. B.*

$$3.\quad \delta\tau = \text{p}-1 \quad \textit{und}$$
$$4.\quad \varkappa\lambda = \delta$$

ist, und man setzt in (1.) *der Reihe nach*

$$5.\quad \text{z} = 1, 2, 3, 4, \ldots \text{p}-1,$$

so bekommt

I. *Der Rest* r *in* (1.) τ *verschiedene Werthe aus den Zahlen* (5.), *und zu jedem dieser* τ *Werthe von* r *gehören* δ *verschiedene und* δ *andere Werthe von* z. *Oder mit andern Worten: die Gleichung* (1.) *hat für jeden der* τ *verschiedenen Werthe, die* r *haben kann,* δ, *und für jedes* r, δ *andere Wurzeln.*

II. *Unter den* τ *verschiedenen Werthen, welche* r *in* (1.) *haben kann, ist immer und für jedes* δ *auch der Werth* r = 1, *und er ge-*

hört immer zu z = 1. *Ist* δ *gerade, so gehört* r = 1 *zugleich zu* z = p − 1, *und ist* δ *ungerade, so gehört zu* z = p − 1 *der Rest* r = p − 1 *oder* r = − 1.

III. *Für* $\delta = p-1$, *also* $\tau = 1$, *kann* r *nur* = 1 *sein, und in diesem Fall drückt die Gleichung* (1.) *den Fermatschen Lehrsatz* (§. 40.) *aus. Es ist also von diesem Satze der gegenwärtige auf gewisse Weise eine Erweiterung.*

IV. *Für* $\delta = \frac{1}{2}(p-1)$, *also* $\tau = 2$, *hat* r *nur die beiden Werthe* 1 *und* p − 1 *oder* = + 1 *und* − 1, *und die zu* r = + 1 *gehörigen* z *sind die Quadratreste, die zu* r = − 1 *gehörigen* z *die Nichtquadratreste zu* p.

V. *Ferner ist*

6. $(p-z)^\delta = \mathfrak{G}p + r$, *wenn* δ *gerade und*

7. $(p-z)^\delta = \mathfrak{G}p - r$, *wenn* δ *ungerade ist.*

Das heifst, wenn δ *gerade ist geben* z *und* p − z *gleiche Reste, und wenn* δ *ungerade ist, sind die Reste, welche* z *und* p − z *geben, zusammen* = p.

VI. *Von den* δ *verschiedenen Werthen von* z, *welche in* (1.) *einen und denselben Rest* r *geben, lassen in* (2.) *je* $\varkappa$ *verschiedene Reste* ϱ, *und je* λ *der Reste* ϱ *sind für ein und dasselbe* r *einander gleich.*

Beispiele. Die weiter unten angehängte mit I. bezeichnete Tafel, welche die sämmtlichen Reste der 1, 2, 3, 4, ... 60 (= $p-1$)ten Potenzen von den Zahlen 1, 2, 3, 4, ... = 60 zu der Stammzahl $p = 61$ enthält, liefert Beispiele zu dem gegenwärtigen und zugleich zu den folgenden Lehrsätzen. Wie solche Tafel mit verhältnifsmäfsig geringer Mühe zu berechnen sei, wird sich weiter unten zeigen.

Zu I. $\delta = 4$ geht in $p - 1 = 60$ auf und giebt $\tau = 15$ (3.). Die Tafel zeigt, dafs für den Exponenten $\delta = 4$, r die $\tau = 15$ verschiedenen Werthe 1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57 und 58 hat und dafs jeder dieser Werthe von r, $\delta = 4$ mal vorkommt.

$\delta = 10$ geht in $p - 1 = 60$ auf und giebt $\tau = 6$ (3.), und für den Exponenten $\delta = 10$ hat nach der Tafel r die $\tau = 6$ verschiedenen Werthe 1, 13, 14, 47, 48 und 60; jeder dieser Werthe von r kommt $\delta = 10$ mal vor.

Zu II. Für *jedes* δ gehört zu $z = 1$ der Rest $r = 1$. Für alle *geraden* δ gehört zu $z = p - 1 = 60$ der Rest $r = 1$ und für alle *ungeraden* δ der Rest $r = p - 1 = 60$ oder $r = -1$.

Zu III. Für $\delta = p - 1 = 60$ sind *alle* r gleich 1; dem Fermatschen Lehrsatze gemäfs.

Zu IV. Für $\delta = 30 = \frac{1}{2}(p-1)$ hat r, wie die Tafel zeigt, nur die beiden Werthe 1 und $p - 1 = 60$. Die zu $r = +1$ gehörigen 30 Werthe

8. 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58 und 60

von z sind die Werthe von r für $\delta = 2$ in der zweiten horizontalen Reihe, also die *Quadratreste* zu p. Die zu $r = p - 1 = 60$ für $\delta = 30$ gehörigen z sind die *übrigen* 30 Zahlen, welche diejenigen (8.) von den Zahlen 1, 2, 3, 4, ... 60 noch übrig lassen, also die *Nichtquadratreste* zu p.

Zu V. Für das *gerade* $\delta = 14$ z. B. giebt nach der Tafel $z = 19$ den Rest $r = 16$ und $p - z = 61 - 19 = 42$ giebt *ebenfalls* den Rest $r = 16$. Für das gerade $\delta = 52$ giebt $z = 26$ den Rest $r = 57$ und $p - z = 61 - 26 = 35$ giebt *ebenfalls* den Rest $r = 57$.

Für das *ungerade* $\delta = 21$ giebt $z = 12$ den Rest $r = 34$ und $p - z = 61 - 12 = 49$ giebt den Rest $r = 27 = p - 34$. Für das ungerade $\delta = 9$ giebt $z = 16$ den Rest $r = 58$ und $p - z = 61 - 16 = 45$ giebt den Rest $r = 3 = p - 58$.

Zu VI. Für $\delta = 20$, also $\tau = 3$ (3.), hat der Rest r die $\tau = 3$ Werthe 1, 13 und 47, und z. B. den Rest $r = 13$ geben die $\delta = 20$ Werthe

9. 4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35, 36, 42, 44, 47, 49, 51 und 57 von z.

Setzt man nun $\lambda = 4$, so ist $\varkappa = 5$ (4.), und sucht man die Reste zur $\lambda = 4$ten Potenz der Werthe (9.) von z auf, so ergiebt sich, dafs

10.
- die $\lambda = 44$ Werthe 4, 17, 4 und 57 von z den Rest $\varrho = 12$,
- - $\lambda = 4$ - - 10, 12, 49 und 51 von z - - $\varrho = 57$,
- - $\lambda = 4$ - - 14, 29, 32 und 47 von z - - $\varrho = 47$,
- - $\lambda = 4$ - - 19, 26, 35 und 42 von z - - $\varrho = 25$,
- und die $\lambda = 4$ - - 25, 30, 31 und 36 von z - - $\varrho = 42$

lassen, also je $\lambda = 4$ der $\delta = 20$ Werthe (9.) von z, die in (1.) zu *einem und demselben* Rest $r (= 13)$ gehören, in (2.) $\varkappa = 5$ verschiedene Reste $\varrho = 12, 57, 47, 25$ und 42; gemäfs (VI.).

Beweis *A*. Nimmt man von (1.) die τte Potenz, so ergiebt sich

11. $$z^{\delta\tau} = (\mathfrak{G}p + r)^\tau = \mathfrak{G}p + r^\tau \text{ (§. 12. 20.)},$$

und da $\delta_\tau = p-1$ (2.), z^{p-1} aber nach (§. 40.) $= \mathfrak{G}p+1$ ist, $\mathfrak{G}p+1 = \mathfrak{G}p+r^\tau$ oder

$$12. \quad r^\tau = \mathfrak{G}p+1.$$

B. Nun ist aber auch eben so wohl, dem Fermatschen Satze zufolge,

$$13. \quad r^{p-1} = \mathfrak{G}p+1;$$

denn r ist jedenfalls eine der Zahlen (5.), welche z sein kann.

Aus (12. und 13.) folgt

$$14. \quad r^\tau - 1 = \mathfrak{G}p \quad \text{und} \quad r^{p-1}-1 = \mathfrak{G}p.$$

Da nun τ in $p-1$ *aufgeht*, so geht auch $r^\tau-1$, wenn man damit $r^{p-1}-1$ dividirt, darin auf und es ist

$$15. \quad r^{p-1}-1 = (r^\tau-1)(r^{(\delta-1)\tau}+r^{(\delta-2)\tau}+r^{(\delta-3)\tau}\ldots\ldots+1) = \mathfrak{G}p.$$

C. In $r^{p-1}-1 = \mathfrak{G}p$ hat, dem Fermatschen Satze zufolge, r ***nothwendig alle*** die $p-1$ verschiedenen Werthe $1, 2, 3, 4, \ldots\ldots p-1$: also mufs für ***alle*** diese Werthe von r auch nothwendig das ***Product*** rechterhand in (15.) mit p aufgehen.

D. Es kann aber der Factor $r^\tau-1$ in (15.) für ***nicht mehr*** als τ verschiedene Werthe von r, und der Factor $r^{(\delta-1)\tau}+r^{(\delta-2)\tau}+r^{(\delta-3)\tau}\ldots\ldots+1$ für ***nicht mehr*** als $(\delta-1)\tau$ verschiedene Werthe von r mit p aufgehen. Denn die Gleichungen

$$16. \quad r^\tau - 1 = \mathfrak{G}p \quad \text{und}$$

$$17. \quad r^{(\delta-1)\tau}+r^{(\delta-2)\tau}+r^{(\delta-3)\tau}\ldots\ldots+1 = \mathfrak{G}p$$

können dem Lehrsatze (§. 44.) zufolge, erstere ***nicht mehr*** als τ, letztere ***nicht mehr*** als $(\delta-1)\tau$ verschiedene Wurzeln haben.

Daraus, und dafs nach (*C.*) die beiden Gleichungen (16. und 17.) ***zusammen*** nothwendig $p-1$ verschiedene Wurzeln haben ***müssen***, folgt, dafs die Gleichung (16.) nothwendig ***gerade*** τ verschiedene Wurzeln haben ***mufs***, und die Gleichung (17.) die übrigen $(\delta-1)\tau$ Wurzeln. Denn hätte (16.) ***weniger*** als τ Wurzeln, so müfste (17.) eben so viele Wurzeln ***mehr*** als $(\delta-1)\tau$ haben, indem $\tau+(\delta-1)\tau = \delta\tau = p-1$ ist; was nach (§. 44.) nicht möglich ist. So kann also (16.) ***nicht weniger*** als τ Wurzeln haben, und nach (§. 44.) auch ***nicht mehr***: also mufs die Zahl der Wurzeln von (16.) nothwendig ***gleich*** τ sein. Auch können (16. und 17.) nicht etwa Wurzeln ***gemeinschaftlich*** haben. Denn hätte z. B. (16.) σ Wurzeln mit (17.) gemeinschaftlich, so könnten in (16. und 17.) überhaupt nur $p-1-\sigma$ ***verschiedene*** Wurzeln vorkommen, da (16. und 17.) ***zusammen*** nur $\tau+(\delta-1)\tau = p-1$ Wurzeln haben können: gleichwohl müssen in (16. und 17.) zusam-

men *alle* die verschiedenen $p-1$ Werthe $1, 2, 3, 4, \ldots p-1$ von r vorkommen, weil dies in (13.) der Fall ist.

Es hat also nothwendig in (12.), und folglich in (11.), woraus (12.) folgt, und mithin auch in (1.), woraus (11.) folgt, der Rest r, τ und *nur* τ verschiedene Werthe >0 und $<p$. Dieses ist was zunächst der Lehrsatz in (I.) behauptet.

E. Es folgt ferner aus

$$18.\quad z^{p-1} = \mathfrak{G}p+1 \text{ (§. 40.) und}$$

$$19.\quad r^{\tau} = \mathfrak{G}p+1 \text{ (12.),}$$

wenn man (19.) von (18.) abzieht,

$$20.\quad z^{p-1} - r^{\tau} = \mathfrak{G}p.$$

Aber τ geht in $p-1$ auf, denn es ist $p-1=\delta\tau$ (3.). Daher geht auch $z^{p-1}-r^{\tau}$ mit $z^{\delta}-r$ *auf* und man erhält, wenn man dividirt, statt (20.):

$$21.\quad z^{\delta\tau}-r^{\tau}=(z^{\delta}-r)(z^{\delta(\tau-1)}+z^{\delta(\tau-2)}r+z^{\delta(\tau-3)}r^2\ldots\ldots+z^{2\delta}r^{\tau-3}+z^{\delta}r^{\tau-2}+r^{\tau-1})$$
$$= \mathfrak{G}p;$$

nemlich, in (21.) die Factoren wiederum multiplicirt, giebt

$$22.\quad z^{\delta\tau}+z^{\delta(\tau-1)}r+z^{\delta(\tau-2)}r^2\ldots\ldots+z^{3\delta}r^{\tau-3}+z^{2\delta}r^{\tau-2}+z^{\delta}r^{\tau-1}$$
$$-z^{\delta(\tau-1)}r-z^{\delta(\tau-2)}r^2\ldots\ldots\ldots\ldots-z^{2\delta}r^{\tau-2}-z^{\delta}r^{\tau-1}-r^{\tau}$$
$$= z^{\delta\tau}-r^{\tau}.$$

F. Da nun die Gleichung (18.) für alle die $p-1$ verschiedenen Werthe $1, 2, 3, 4, \ldots p-1$ von z gilt, so mufs auch (21.) *alle* diese Werthe von z zulassen, und folglich müssen die beiden Factoren rechterhand in (21.) für *alle* diese verschiedenen Werthe von z mit p aufgehen.

G. Ganz so wie in (*D.*) folgte, dafs die beiden Factoren rechterhand in (15.) nothwendig, der eine τ, der andere $(\delta-1)\tau$ verschiedene Werthe von r zulassen müssen, folgt auch hier, dafs die beiden Factoren rechterhand in (21.), der eine nothwendig für δ, der andere für $\delta(\tau-1)$ verschiedene Werthe von z gelten müssen, denn die Gleichungen

$$23.\quad z^{\delta}-r = \mathfrak{G}p \text{ und}$$

$$24.\quad z^{\delta(\tau-1)}+z^{\delta(\tau-2)}r+z^{\delta(\tau-r)}r^2\ldots\ldots+z^{2\delta}r^{\tau-3}+z^{\delta}r^{\tau-2}+r^{\tau-1} = \mathfrak{G}p$$

können nach (§. 44.), die erste *nicht mehr* als δ, die zweite *nicht mehr* als $\delta(\tau-1)$ verschiedene Wurzeln haben.

Also folgt aus der Gleichung (23.), welche diejenige (1.) selbst ist, dafs zu jedem Werth, welchen r haben kann, und deren es nach (*D.*) τ giebt,

z nothwendig δ verschiedene Werthe hat. Und zwar müssen jedem *andern r*, δ *andere z* entsprechen: denn gehörten zu *verschiedenen r gleiche z*, so würden, indem nur τ verschiedene r vorhanden sind, *nicht alle* $p-1=\delta\tau$ verschiedene Werthe von z vorkommen; was gleichwohl in (21.) oder (18.) der Fall sein mufs.

Dieses ist was der Lehrsatz weiter in (I.) behauptet.

H. Für *jedes* δ giebt in (1.) $z=1$, $r=1$. Für jedes *gerade* δ giebt (1.) $(p-1)^\delta=\mathfrak{G}p+1$, also $r=1$; für jedes *ungerade* δ giebt (1.) $(p-1)^\delta=\mathfrak{G}p-1$, also $r=p-1$ oder $r=-1$. Dieses ist was (II.) behauptet.

I. Für $\delta=p-1$ giebt (1.), dem Fermatschen Lehrsatze (§. 40.) gemäfs, für *jedes z*, $z^{p-1}=\mathfrak{G}p+1$; gemäfs (III.).

K. Für $\delta=\frac{1}{2}(p-1)$ giebt (1.), wenn man für z die *Quadratreste* zu p setzt, zufolge (§. 49.), $z^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$, und wenn man für z die *Nichtquadratreste* zu p setzt, zufolge (§. 49. 2.), $z^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$; gemäfs (IV.).

L. Setzt man in (1.) $p-z$ statt z, so ergiebt sich

25. $(p-z)^\delta=\mathfrak{G}p+(-z)^\delta=\mathfrak{G}p\pm(\mathfrak{G}p+r)\,(1.)=\mathfrak{G}p\pm r,$

je nachdem δ *gerade* oder *ungerade* ist; gemäfs (6. und 7. V.).

M. Aus (2.) folgt, wenn man die $\varkappa$ten Potenzen davon nimmt,

26. $z^{\varkappa\lambda}=\mathfrak{G}p+\varrho^\varkappa=z^\delta$ (4.),

also ist, gemäfs (1.),

$$\mathfrak{G}p+r=\mathfrak{G}p+\varrho^\varkappa \text{ oder}$$

27. $\varrho^\varkappa=\mathfrak{G}p+r,$

mithin hat ϱ, zufolge (I.), für *ein* und *dasselbe r*, $\varkappa$ *verschiedene* Werthe aus denen von z, welche in (1.) das bestimmte r geben. Andrerseits gehören in (2.), ebenfalls gemäfs (I.), λ verschiedene Werthe von z zu einem und demselben ϱ; und da nun alle die Werthe von ϱ aus denjenigen Werthen von z sind, die in (1.) ein und dasselbe r geben, so gehören λ *dieser* Werthe von z zu einem und demselben r. Dieses zusammen behauptet (VI.).

Anm. *N.* Der Beweis beruht auf einer Verbindung der Sätze (§. 40. 43. und 44.). Wie in (§. 51.) sind hier die Schlüsse in (*D.* und *G.*) eigenthümlich.

§. 55.

Lehrsatz.

Es sei in den Zahlengleichungen

$$1.\quad z^{\varepsilon} = \mathfrak{G}p + r \text{ und}$$

$$2.\quad z^{\sigma} = \mathfrak{G}p + \varrho$$

p *eine Stammzahl*, $r > 0$ *und* $< p$ *und der Reihe nach*

$$3.\quad z = 1, 2, 3, 4, \ldots p - 1.$$

I. *Sind in* (1.) *und* (2.) ε *und* σ *zu einander* ***theilerfremd***, *gleichviel ob auch zu* $p-1$, *oder nicht, so geben diejenigen Werthe von* z *aus denen* (3.), *zu welchen in* (1.) ***gleiche*** r *gehören, in* (2.) ***nicht zugleich gleiche*** ϱ; *und umgekehrt.*

II. *Ist in* (1.) ε *zu* $p-1$ ***theilerfremd***, *so bekommt* r *zu jedem andern Werth von* z *einen* ***andern*** *Werth, und die Werthe von* r *durchlaufen, eben wie* z *selbst, alle die Zahlen* 1, 2, 3, 4, ... $p-1$, *obwohl in verschiedener Ordnung.*

III. *Ferner ist in* (1.)

$$4.\quad (p - z)^{\varepsilon} = \mathfrak{G}p + r \text{ für gerade } \varepsilon \text{ und}$$

$$5.\quad (p - z)^{\varepsilon} = \mathfrak{G}p - r \text{ für ungerade } \varepsilon;$$

das heifst, wenn z *zu* p *den Rest* r *läfst, so gehört für ein* ***gerades*** ε *zu* $p-z$ ***derselbe Rest*** r *und für ein* ***ungerades*** ε *der Rest* $-r$ *oder* $p-r$.

IV. *Ist* δ *der* ***gröfste Gemeintheiler*** *von* ε *und* $p-1$ *und*

$$6.\quad \varepsilon = \eta\delta, \quad p - 1 = \tau\delta,$$

so bekommt r *in* (1.) *je für* δ *und für nicht mehrere verschiedene Werthe von* z *aus denen* (3.) ***denselben*** *Werth, und für die* ***sämmtlichen*** z (3.) τ ***verschiedene*** *Werthe.*

V. *Ist* λ *irgend ein* ***Gemeintheiler*** *von* ε *und* σ *und zugleich ein* ***Theiler*** *von* $p-1$, *z. B.*

$$7.\quad \varepsilon = \varkappa\lambda, \quad \sigma = \omega\lambda \quad \text{und} \quad p - 1 = \zeta\lambda,$$

so gehören zu den nemlichen je λ *Werthen von* z *aus denen* (3.), *welche in* (1.) ***gleiche*** r *geben, auch in* (2.) ***gleiche*** ϱ, *und in dem Fall, wenn* ϰ *und* ω *zu einander* ***theilerfremd*** *sind,* ***nicht mehrere.***

Beispiele (aus Taf. I.). Zu I. $\sigma = 21$ und $\varepsilon = 50$ sind zu einander *theilerfremd*, aber beide *nicht* zu $p-1 = 60$. Die 3 Werthe 7, 24 und 30 von *z*, welche für $\sigma = 21$ den Rest $\varrho = 24$ lassen, geben für $\varepsilon = 50$ die Reste $r = 14$, 60 und 48, also *andere* Reste; gemäfs (I.).

$\sigma = 18$ und $\varepsilon = 49$ sind zu einander *theilerfremd*, aber nur ε ist es zugleich zu $p - 1 = 60$. Die 6 Werthe 4, 5, 9, 52, 56 und 57 von z, welche für $\sigma = 18$ den Rest $\varrho = 58$ lassen, geben für $\varepsilon = 49$ die Reste 49, 46, 34, 27, 15 und 12, also *andere* Reste; gemäfs (I.).

$\sigma = 13$ und $\varepsilon = 49$ sind zu einander und zugleich *beide* zu $p - 1 = 60$ *theilerfremd*. Der Werth 3 von z, welcher für $\sigma = 13$ den Rest $\varrho = 27$ läfst, giebt für $\varepsilon = 49$ den Rest $r = 41$, also einen *andern* Rest; gemäfs (I.).

Zu II. Die Zahlen

8. $\varepsilon = 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53$ und $59 > 1$

sind zu $p - 1 = 60$ *theilerfremd*; und für *alle* diese Werthe ε des Exponenten der z in (1.) hat r, wie es die Tafel zeigt, für jeden andern Werth von z einen *andern* Werth. Die Werthe von r durchlaufen, eben wie die z selbst, alle die Zahlen 1, 2, 3, 4, ... $p - 1$, obwohl in verschiedener Ordnung; gemäfs (II.).

Zu III. Für das *gerade* $\varepsilon = 38$ ist z. B. für $z = 13$, $r = 47$, und für $z = 48 = p - 13$ ist r ebenfalls $= 47$; gemäfs (4.).

Für das *ungerade* $\varepsilon = 53$ ist z. B. für $z = 16$, $r = 57$ und für $z = 45 = p - 16$ ist $r = 4 = p - 57$; gemäfs (5.).

Zu IV. Es sei $\varepsilon = 42$, so ist der gröfste Gemeintheiler von ε in $p - 1 = 60$, $\delta = 6$ und in (6.) $\eta = 7$, $\tau = 10$. In der Tafel findet sich, dafs für die εte $= 42$te Potenz der z, z. B. die $\delta = 6$ Werthe 3, 19, 22, 38, 42 und 51 von z einen und denselben Rest $r = 9$ geben: und für die *sämmtlichen* z (3.) hat r die $\tau = 10$ verschiedenen Werthe 1, 3, 9, 20, 27, 34, 41, 52, 58 und 60; gemäfs (IV.).

Zu V. Der Gemeintheiler $\lambda = 6$ zu $\varepsilon = 24$ und $\sigma = 48$ ist zugleich ein Theiler von $p - 1 = 60$. Die $\lambda = 6$ Werthe 4, 5, 6, 9, 17, 23 von z geben für $\varepsilon = 24$ den Rest $r = 34$. *Dieselben* Werthe von z geben zu $z^\sigma = z^{48}$ alle den Rest $\varrho = 58$; gemäfs (V.).

Ein Gemeintheiler zu $\varepsilon = 24$ und $\sigma = 45$ ist $\lambda = 3$, was zugleich in $p - 1 = 60$ aufgeht. Dabei ist $\varkappa = 8$ und $\omega = 15$, und diese Werthe von $\varkappa$ und ω sind zu einander *theilerfremd*. Die 12 Werthe 2, 3, 19, 22, 26, 28, 33, 35, 39, 42, 58 und 59 von z geben für $\varepsilon = 24$ den Rest $\varrho = 20$ und für $\sigma = 45$ die Reste 50, 60, 60, 1, 50, 11, 50, 11, 60, 1, 1 und 11, und nur je $\lambda = 3$ von den letztern sind wieder gleich; gemäfs (V.).

Beweis A. Von den beiden Exponenten ε und σ in (1. und 2.) bezeichne ε den *gröfsern*. Man setze

$$9. \begin{cases} \varepsilon = m\sigma + \sigma, \\ \sigma = m_1\sigma + \sigma_2, \\ \sigma_1 = m_2\sigma_2 + \sigma_3, \\ \sigma_2 = m_3\sigma_3 + \sigma_4, \\ \dots\dots\dots \\ \sigma_{n-2} = m_{n-1}\sigma_{n-1} + \sigma_n, \end{cases}$$

wo $\sigma_1 < \sigma$, $\sigma_2 < \sigma_1$, $\sigma_3 < \sigma_2$, ... sein sollen.

a. Da ε und σ zu einander *theilerfremd* sein sollen, so führt (9.) nach (§. 19. IV.) *nothwendig* zuletzt auf den Rest $\sigma_n = 1$.

b. Es seien a und b zwei von den Werthen von z, welche nach der Voraussetzung in (1.) *gleiche Reste* r lassen, so dafs also

$$10.\quad a^\varepsilon = \mathfrak{S}p + r \quad \text{und} \quad b^\varepsilon = \mathfrak{S}p + r$$

ist. Könnten nun diese *nemlichen* Werthe a und b von z auch in (2.) *gleiche* Reste ϱ lassen, so müfste auch

$$11.\quad a^\sigma = \mathfrak{S}p + \varrho \quad \text{und} \quad b^\sigma = \mathfrak{S}p + \varrho$$

sein.

c. Drückt man in (10.) ε nach der ersten der Gleichungen (9.) aus, so ergiebt sich

$$a^{m\sigma+\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad b^{m\sigma+\sigma_1} = \mathfrak{S}p + r \quad \text{oder}$$

$$12.\quad a^{m\sigma}a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad b^{m\sigma}b^{\sigma_1} = \mathfrak{S}p + r,$$

und da nach (11.)

$$13.\quad a^{m\sigma} = \mathfrak{S}p + \varrho^m \quad \text{und} \quad b^{m\sigma} = \mathfrak{S}p + \varrho^m$$

ist (§. 12. 20.),

$$(\mathfrak{S}p + \varrho^m)a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad (\mathfrak{S}p + \varrho^m)b^{\sigma_1} = \mathfrak{S}p + r \quad \text{oder}$$

$$14.\quad \varrho^m a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad \varrho^m b^{\sigma_1} = \mathfrak{S}p + r.$$

d. Die Gleichungen (14.) von einander abgezogen, geben

$$15.\quad \varrho^m(a^{\sigma_1} - b^{\sigma_1}) = \mathfrak{S}p,$$

oder, wenn man

$$16.\quad a^{\sigma_1} = \mathfrak{S}p + a_1 \quad \text{und} \quad b^{\sigma_1} = \mathfrak{S}p + b_1$$

setzt, wo $a_1 < p$ und $b_1 < p$ angenommen wird,

$$\varrho^m(\mathfrak{S}p + a_1 - \mathfrak{S}p - b_1) = \mathfrak{S}p \quad \text{oder}$$

$$17.\quad \varrho^m(a_1 - b_1) = \mathfrak{S}p:$$

also müfste entweder ϱ oder $a_1 - b_1$ mit p *aufgehen*. Da beides nicht der Fall ist, indem ϱ, a_1 und b_1 alle drei $< p$ sind, so kann die Gleichung (17.)

nur erfüllt werden, wenn $a_1 - b_1 = 0$ oder

$$18. \quad a_1 = b_1$$

ist. Folglich können die beiden Werthe a und b von z, die nach der Voraussetzung in (1.) *gleiche* Reste r lassen, nur dann auch in (2.) *gleiche* Reste ϱ geben, wenn in (16.) $a_1 = b_1$ ist.

e. Die Gleichungen (11.), nach der zweiten Gleichung in (9.) ausgedrückt, geben

$$a^{m_1\sigma_1+\sigma_2} = \mathfrak{G}p + \varrho \quad \text{und} \quad b^{m_1\sigma_1+\sigma_2} = \mathfrak{G}p + \varrho \quad \text{oder}$$

$$19. \quad a^{m_1\sigma_1}a^{\sigma_2} = \mathfrak{G}p + \varrho \quad \text{und} \quad b^{m_1\sigma_1}b^{\sigma_2} = \mathfrak{G}p + \varrho,$$

oder, da vermöge (16.)

$$20. \quad a^{m_1\sigma_1} = \mathfrak{G}p + a_1^{m_1} \quad \text{und} \quad b^{m_1\sigma_1} = \mathfrak{G}p + b_1^{m_1}$$

ist (§. 12. 20.),

$$(\mathfrak{G}p + a_1^{m_1})a^{\sigma_2} = \mathfrak{G}p + \varrho \quad \text{und} \quad (\mathfrak{G}p + b_1^{m_1})b^{\sigma_2} = \mathfrak{G}p + \varrho \quad \text{oder}$$

$$21. \quad a_1^{m_1}a^{\sigma_2} = \mathfrak{G}p + \varrho \quad \text{und} \quad b_1^{m_1}b^{\sigma_2} = \mathfrak{G}p + \varrho,$$

oder auch, da nach (18.) $a_1 = b_1$ sein mufs,

$$22. \quad a_1^{m_1}a^{\sigma_2} = \mathfrak{G}p + \varrho \quad \text{und} \quad a_1^{m_1}b^{\sigma_2} = \mathfrak{G}p + \varrho.$$

f. Die Gleichungen (22.) von einander abgezogen, geben

$$23. \quad a_1^{m_1}(a^{\sigma_2} - b^{\sigma_2}) = \mathfrak{G}p,$$

oder, wenn man

$$24. \quad a^{\sigma_2} = \mathfrak{G}p + a_2 \quad \text{und} \quad b^{\sigma_2} = \mathfrak{G}p + b_2$$

setzt, wo $a_2 < p$ und $b_2 < p$ angenommen wird,

$$a_1^{m_1}(\mathfrak{G}p + a_2 - \mathfrak{G}p - b_2) = \mathfrak{G}p \quad \text{oder}$$

$$25. \quad a_1^{m_1}(a_2 - b_2) = \mathfrak{G}p:$$

also müfste entweder a_1 oder $a_2 - b_2$ mit p *aufgehen*. Da beides nicht der Fall ist, indem a_1, a_2 und b_2 alle drei $< p$ sind, so kann die Gleichung (25.) nur erfüllt werden, wenn $a_2 - b_2 = 0$ oder

$$26. \quad a_2 = b_2$$

ist. Folglich können die beiden Werthe a und b von z, die nach der Voraussetzung (in 1.) *gleiche* Reste r lassen, nur dann auch in (2.) *gleiche* Reste ϱ geben, wenn, nächst $a_1 = b_1$ in (16.), auch in (24.) $a_2 = b_2$ ist.

g. Die Gleichungen (16.) sind, da $a_1 = b_1$ sein mufs (18.),

$$27. \quad a^{\sigma_1} = \mathfrak{G}p + a_1 \quad \text{und} \quad b^{\sigma_1} = \mathfrak{G}p + a_1.$$

Verfährt man mit diesen Gleichungen von neuem ganz so wie in (*c.* und *d.*) mit den Gleichungen (11.), und zwar indem man den Exponenten σ_1 in (27.) nach der *dritten* Gleichung (9.) ausdrückt, so ergiebt sich, wie leicht zu sehen, indem nur alle *Zeiger* um 1 erhöht werden dürfen, dafs, wenn man,

ähnlich wie in (24.),

28. $a^{\sigma_3} = \mathfrak{G}p + a_3$ und $b^{\sigma_3} = \mathfrak{G}p + b_3$

setzt, auch wieder, ähnlich wie in (26.),

29. $a_3 = b_3$

sein mufs, wenn die Gleichungen (27.) und folglich die Gleichungen (11.) Statt finden sollen.

h. Auf dieselbe Weise folgt weiter, dafs

30. $$\begin{cases} \text{Für } a^{\sigma_4} = \mathfrak{G}p + a_4 \text{ und } b^{\sigma_4} = \mathfrak{G}p + b_4, \; a_4 = b_4; \\ \text{Für } a^{\sigma_5} = \mathfrak{G}p + a_5 \text{ und } b^{\sigma_5} = \mathfrak{G}p + b_5, \; a_5 = b_5; \\ \quad \text{und so weiter; zuletzt also dafs} \\ \text{Für } a^{\sigma_n} = \mathfrak{G}p + a_n \text{ und } b^{\sigma_n} = \mathfrak{G}p + b_n, \; a_n = b_n \end{cases}$$

sein mufs, wenn die Gleichungen (11.) Statt finden sollen, das heifst, wenn zwei Werthe a und b von z, die in $z^\varepsilon = \mathfrak{G}p + r$ (1.) *gleiche* Reste r zu p lassen, auch in $z^\sigma = \mathfrak{G}p + \varrho$ (2.) zu p *gleiche* Reste ϱ geben sollen.

i. Nun ist aber $\sigma_n = 1$ (*a.*), also geben die letzten der Gleichungen (30.)

$a^1 = \mathfrak{G}p + a_n$ und $b^1 = \mathfrak{G}p + b_n$ oder

31. $a_n = a$ und $b_n = b$.

Die letzte Bedingung $a_n = b_n$ in (30.) für das Stattfinden der Gleichungen (11.) wäre also

32. $a = b$.

Diese Bedingung wird *nicht* erfüllt, indem a und b nicht *gleiche* sondern *ungleiche* Werthe von z ausdrücken. Also können die Gleichungen (11.) *nicht* Statt finden: das heifst, keine zwei Werthe a und b von z, und folglich auch überhaupt nicht diejenigen Werthe von z, welche in $z^\varepsilon = \mathfrak{G}p + r$ (1.) zu p *gleiche* Reste r lassen, können zugleich in $z^\sigma = \mathfrak{G}p + \varrho$ (2.) zu p *gleiche* Reste ϱ geben, sobald ε und σ zu einander *theilerfremd* sind. Ob ε und σ zu $p-1$ theilerfremd sind, oder nicht, kommt bei dem Beweise nicht in Betracht.

Dieses ist es, was der Lehrsatz in (I.) behauptet.

B. Wenn in (2.) $\sigma = p - 1$ ist, so geben *alle* die Werthe (3.) von z nach dem Fermatschen Lehrsatze (§. 40.) *gleiche* Reste ϱ, nemlich *alle* den Rest $\varrho = 1$. Nun geben nach (I.) alle die Werthe von z, die in (2.) *gleiche* Reste ϱ lassen, in (1.) *nicht* gleiche Reste r. Also geben in dem gegenwärtigen Fall *alle* die Werthe (3.) von z in (1.) sämmtlich *verschiedene* Werthe von r. Und folglich mufs, da $p-1$ Werthe von z und folglich von r vorhanden und alle > 0 und $< p$ sind, r, eben wie z, alle die Zahlen (3.) durchlaufen. Dies behauptet (II.).

C. Es ist

$$33.\quad (p-z)^\varepsilon = \mathfrak{S}p + (-z)^\varepsilon = \mathfrak{S}p + z^\varepsilon(-1)^\varepsilon$$

und, da $z^\varepsilon = \mathfrak{S}p + r$ ist (1.),

$$34.\quad (p-z)^\varepsilon = \mathfrak{S}p + (\mathfrak{S}p + r)(-1)^\varepsilon = \mathfrak{S}p + r(-1)^\varepsilon.$$

Dieses giebt

$$35.\quad (p-z)^\varepsilon = \mathfrak{S}p + r, \text{ wenn } \varepsilon \textit{ gerade} \text{ und}$$

$$36.\quad (p-z)^\varepsilon = \mathfrak{S}p - r, \text{ wenn } \varepsilon \textit{ ungerade} \text{ ist;}$$

gemäfs (III.).

D. a. Setzt man für (IV.), wo δ einer der Theiler von $p-1$ sein soll,

$$37.\quad z^\delta = \mathfrak{S}p + r_1,$$

so geben nach (§. 54. I.) δ verschiedene Werthe von z, und nicht mehrere, ***denselben*** Rest r_1.

Da nun $\eta\delta = \varepsilon$ sein soll (6.), so giebt (37.)

$$38.\quad z^{\eta\delta} \text{ oder } z^\varepsilon = \mathfrak{S}p + r_1^\eta \text{ (§. 12. 20.)}$$

und, da $z^\varepsilon = \mathfrak{S}p + r$ sein soll (1.),

$$\mathfrak{S}p + r = \mathfrak{S}p + r_1^\eta \text{ oder}$$

$$39.\quad r_1^\eta = \mathfrak{S}p + r.$$

Nun geben δ verschiedene und nicht mehrere Werthe von z in (37.) ***denselben*** Rest r_1, also geben sie auch vermöge (39.) denselben Werth r für (2.).

b. Aber obgleich nicht mehre als δ Werthe von z in (37.) denselben Rest r_1 lassen, fragt es sich doch, ob nicht dennoch etwa andere Werthe von z nach (39.) für (1.) gleiche Reste r geben.

Andere als diejenigen δ Werthe von z, welche in (37.) dasselbe r_1 geben, lassen nothwendig in (37.) einen ***andern*** Rest r_2, so dafs für sie

$$40.\quad z^\delta = \mathfrak{S}p + r_2$$

ist. Sollte nun dieser Werth von z dennoch in (2.) denselben Rest r lassen, so müfste gemäfs (39.)

$$41.\quad r_2^\eta = \mathfrak{S}p + r$$

sein; also müfste die ηte Potenz zweier ***verschiedenen*** Zahlen r_1 und r_2, beide >0 und $<p$, zu p den ***gleichen*** Rest r lassen. Dieses aber ist nach (II.) nicht möglich, indem δ der ***gröfste*** Gemeintheiler von ε und $p-1$ sein soll, also η zu $p-1$ ***theilerfremd*** ist. Also lassen ***nicht mehr*** als δ verschiedene Werthe von z in (1.) ***denselben*** Rest r, sobald δ der ***gröfste*** Gemeintheiler von ε und $p-1$ ist. Mithin giebt es dann auch in (1.) in diesem

Falle nur $\frac{p-1}{\delta}=\tau$ (6.) *verschiedene* Werthe von r. Dieses zusammen behauptet (IV.).

E. a. In (V.) soll λ ein Theiler von $p-1$ sein. Dieserhalb geben zufolge (§. 54. I.), wenn man

$$42.\quad z^{\lambda}=\mathfrak{G}p+r_1$$

setzt, λ verschiedene Werthe von z das *gleiche* r_1.

Da nun $\varepsilon=\varkappa\lambda$ und $\sigma=\omega\lambda$ sein soll (7.), so giebt (42.)

$$43.\quad z^{\varkappa\lambda} \text{ oder } z^{\varepsilon}=\mathfrak{G}p+r_1^{\varkappa}=\mathfrak{G}p+r \text{ (1.) und}$$

$$44.\quad z^{\omega\lambda} \text{ oder } z^{\sigma}=\mathfrak{G}p+r_1^{\omega}=\mathfrak{G}p+\varrho \text{ (2.);}$$

und folglich sind für je λ verschiedene Werthe von z die Werthe von $r_1^{\varkappa}$ und r_1^{ω} und folglich von r in (1.) und ϱ in (2.) einander gleich.

b. Sind $\varkappa$ und ω zu einander *theilerfremd,* so folgt, eben wie in (*D. b.*), dafs nicht auch noch andere als die λ Werthe von z in (1. und 2.) ebenfalls gleiche r und *zugleich* gleiche ϱ geben können.

F. Anm. Ein Hauptmoment des Beweises ist (*A.*), nemlich, dafs man, wenn ε und σ zu einander *theilerfremd* sind, nach (§. 19. IV.) nothwendig auf den Rest $\sigma_n=1$ kommt. Sonst beruht der Beweis auf (§. 40. und 54.).

§. 56.

Lehrsatz.

I. *Es giebt für jede Stammzahl* p *immer Werthe von* $z>0$ *und* $<p$, *aufser* $z=1$, *von welchen schon niedrigere Potenzen als die* z^{p-1}, *welche nach dem Fermatschen Lehrsatze* (§. 40.) *zu* p *immer den Rest* 1 *läfst, ebenfalls schon diesen Rest geben, so dafs also die Gleichung*

$$1.\quad z^{\varepsilon}=\mathfrak{G}p+1$$

für diese oder jene z *auch schon für* $\varepsilon<p-1$ *Statt findet.*

II. *Die Werthe von* $\varepsilon<p-1$, *für welche* (1.) *Statt findet, sind alle diejenigen Zahlen* $<p-1$, *welche mit* $p-1$ *einen Theiler* δ *gemein haben, so dafs etwa*

$$2.\quad \varepsilon=\delta\eta \text{ und } p-1=\delta\tau$$

sein mufs.

III. *Für solche Werthe von* ε *findet die Gleichung* (1.), *wenn* δ *den gröfsten Gemeintheiler von* ε *und* $p-1$ *bezeichnet, für* δ *und für nicht mehr verschiedene Werthe von* z *Statt.*

IV. ***Für alle ε, die mit*** p — 1 ***keinen Theiler*** $>$ 1 ***gemein haben, findet die Gleichung*** (1.) ***nur für den einzigen Werth*** 1 ***von*** z ***Statt.***

V. ***Die Werthe von ε, für welche die Gleichung*** (2.) ***Statt findet, sind aber keineswegs immer die kleinsten, sondern es kann, wenn*** (1.) ***von irgend einem*** z ***erfüllt wird, auch für einen noch kleineren Werth von ε schon, für dasselbe*** z, $z^{\varepsilon} = \mathfrak{G}p + 1$ ***sein.***

Beispiele (aus Taf. I.). Zu I. Wie die Tafel zeigt ist z. B. schon $13^3 = \mathfrak{G}p + 1$, $11^4 = \mathfrak{G}p + 1$, $9^5 = \mathfrak{G}p + 1$ u. s. w.

Zu II. Die Zahlen $< p - 1$, welche mit $p - 1 = 60$ einen Theiler > 1 gemein haben, sind folgende:

$$3. \quad \begin{cases} 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, \\ 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58. \end{cases}$$

Für alle diese Werthe des Exponenten ε kommt, wie die Tafel zeigt, unter den Werthen von r schon der Rest 1 vor.

Zu III. Der ***gröfste*** Gemeintheiler von ε und $p - 1$ ist z. B. für $\varepsilon = 55$, $\delta = 5$, und der Tafel zufolge wird die Gleichung (1.) für die $\delta = 5$ Werthe 1, 9, 20, 34 und 58 von z erfüllt.

Zu IV. Für $\varepsilon = 7$, 11, 13, 49 etc., die mit $p - 1$ ***keinen*** Theiler > 1 gemein haben, wird die Gleichung (1.), wie die Tafel zeigt, nur durch den einzigen Werth 1 von z erfüllt.

Zu V. Es ist $9^{45} = \mathfrak{G}p + 1$, aber auch schon 9^5, 9^{10}, 9^{15} u. s. w. ist $= \mathfrak{G}p + 1$.

Beweis ***A.*** Man setze

$$4. \quad z^{\tau} = \mathfrak{G}p + r,$$

wo $r > 0$ und $< p$, so ist

$$5. \quad z^{\tau\delta} = \mathfrak{G}p + r^{\delta} \text{ (§. 12. 20.)},$$

und da

$$6. \quad z^{\tau\delta} = z^{p-1} \text{ (2.)} = \mathfrak{G}p + 1 \text{ (§. 40.)}$$

ist, so ist aus (5. und 6.)

$$\mathfrak{G}p + r^{\delta} = \mathfrak{G}p + 1 \text{ oder}$$

$$7. \quad r^{\delta} = \mathfrak{G}p + 1,$$

so wie auch

$$8. \quad r^{\delta\eta} = (\mathfrak{G}p + 1)^{\eta} = \mathfrak{G}p + 1^{\eta} = \mathfrak{G}p + 1 = r^{\varepsilon}.$$

Nun sind δ und $\varepsilon < p-1$, also giebt es immer Zahlen $r > 0$ und $< p-1$, und folglich Werthe von z, von welchen schon *niedrigere* als die $p-1$te Potenz zu p den Rest 1 lassen; gemäfs (I.).

B. Was in (*A.*) bewiesen, gilt für *jeden* Theiler δ von $p-1$, also auch für jedes ε, welches mit $p-1$ irgend einen Theiler $\delta > 1$ gemein hat. Gemäfs (II.).

C. Die Gleichung (7.) findet nach (§. 54. I.) hier für den bestimmten Werth 1 des Restes für δ und für nicht mehr verschiedene Werthe von z (hier r) Statt; also wenn δ der *gröfste* Gemeintheiler von ε und $p-1$ ist, auch für δ verschiedene Werthe, mithin auch die Gleichung (8.) oder (1.) für eben so viele Werthe, und für nicht mehrere. Gemäfs (III.).

D. Hat ε keinen Theiler >1 mit $p-1$ gemein, so durchläuft nach (§. 55. II.) in

$$9. \quad z^{\varepsilon} = \mathfrak{G}p + r$$

r alle die Zahlen $1, 2, 3, 4, \ldots. \; p-1$: also findet die Gleichung (1.) in diesem Fall nur für den einzigen Werth 1 von z Statt; gemäfs (IV.).

E. Nach (II.) giebt es Werthe von $z > 1$, die für jeden *Theiler* δ von $p-1$ die Gleichung

$$10. \quad z^{\delta} = \mathfrak{G}p + 1$$

erfüllen. *Dieselben* Werthe von z erfüllen aber auch die Gleichung

$$11. \quad z^{\delta\eta} = z^{\varepsilon} = \mathfrak{G}p + 1;$$

denn (10.) giebt

$$12. \quad z^{\delta\eta} = (\mathfrak{G}p + 1)^{\eta} = \mathfrak{G}p + 1^{\eta} = \mathfrak{G}p + 1.$$

Also die z, welche die Gleichung (1.) erfüllen, können auch schon der Gleichung (10.) genugthun, in welcher $\delta < \varepsilon$ ist.

Anm. *F.* Die gegenwärtigen Sätze beruhen auf (§. 54. und 55.).

§. 57.
Erklärung.

Zufolge (§. 56.) giebt es, wenn p eine *Stammzahl* ist, immer Werthe von $z > 1$, von welchen schon *niedrigere* Potenzen, als nach dem Fermatschen Satze die Potenz z^{p-1}, zu p den Rest 1 lassen, also immer *Wurzeln* > 1 zu der Gleichung

$$1. \quad z^{\varepsilon} = \mathfrak{G}p + 1,$$

wo $\varepsilon < p - 1$.

Nun giebt es auch offenbar immer *niedrigste* Exponenten λ, für welche, für bestimmte z,

$$2. \quad z^{\lambda} = \mathfrak{G}p + 1$$

ist.

Die Wurzeln z *dieser* Gleichung, für den *niedrigsten* Exponenten λ, die also für alle *kleineren* Exponenten 1, 2, 3, ... bis $\lambda - 1$ *andere* Reste als 1 und *zuerst* für den Exponenten λ den Rest 1 geben, sollen *Stammwurzeln aus* 1 *zu p für den Exponenten* λ, oder kürzer, *λte Stammwurzeln aus* 1 *zu p* heifsen und durch z_{λ} bezeichnet werden.

Ist λ gleich $p - 1$ selbst, so dafs also *alle niedrigere* Potenzen als z^{p-1} andere Reste als 1 zu p lassen, so sollen die z, welche diese Eigenschaft haben, *Hauptstammwurzeln aus* 1 *zu p* heifsen.

Gewöhnlich giebt man nur den *Hauptstammwurzeln* einen besondern Namen; man nennt sie *primitive Wurzeln*. Es ist aber gut, auch den übrigen Stammwurzeln, für welche $\varepsilon < p - 1$ ist, eine besondere Benennung beizulegen; und die Benennungen *Stammwurzel*, und für den Fall $\varepsilon = p - 1$ *Hauptstammwurzel*, scheinen passend, wenigstens nicht minder passend zu sein, als die nicht deutsche Benennung für letztere.

Wenn in der Gleichung

$$3. \quad z^{x} = \mathfrak{G}p + r$$

z eine *Hauptstammwurzel* und $x < p - 1$, also r zufolge der Eigenschaft der Stammwurzeln *nicht* $= 1$ ist, so nennt man auch den Exponenten x, für welchen der Rest r Statt findet, *Index* zu r.

§. 58.

Lehrsatz.

I. ***Es giebt, wenn*** p ***eine Stammzahl ist, zu jedem Exponenten*** $\delta > 1$, ***der in*** $p-1$ ***aufgeht, also auch zu*** $p-1$ ***selbst, Stammwurzeln; das heifst Werthe von*** z, ***von welchen keine niedrigere Potenz als*** z^δ ***zu*** p ***den Rest*** 1 ***läfst, also für welche für keinen kleineren Exponenten als*** δ

$$1. \quad z^\delta = \mathfrak{G}p+1$$

ist.

II. ***Zu Exponenten*** δ, ***die nicht in*** $p-1$ ***aufgehen, gleichviel ob sie mit*** $p-1$ ***Theiler gemein haben, oder nicht, giebt es keine Stammwurzeln.***

Beispiel. (Aus Taf. I.) $z=1$, 13 und 47 sind die ***Stammwurzeln*** zu dem Theiler $\delta=4$ von $p-1=60$. $z=3$, 27, 41 und 52 sind die ***Stammwurzeln*** zu dem Theiler $\delta=10$ von $p-1$, und $z=8$, 23, 24, 28, 33, 37, 38 und 53 sind die ***Stammwurzeln*** zu dem Theiler $\delta=20$ von $p-1$ u. s. w. $z=2$, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55 und 59 sind die ***Hauptstammwurzeln*** oder diejenigen zu $\delta=p-1=60$.

Beweis von I. ***A.*** Nach (§. 56. III.) giebt es für jeden Theiler δ von $p-1$, δ verschiedene Werthe von z, so wie nach (§. 40.) für δ ***gleich*** $p-1$, $p-1$ verschiedene Werthe von z, für welche

$$2. \quad z^\delta = \mathfrak{G}p+1$$

ist.

B. Giebt nun in der Gleichung (2.) keine der verschiedenen Potenzen $z^1, z^2, z^3, \dots z^{\delta-1}$ zu p den Rest 1, sondern erst z^δ selbst, so ist z in (2.) ***selbst*** die δte ***Stammwurzel*** aus 1 zu p.

Geben aber schon niedrigere Potenzen als z^δ zu p den Rest 1, so wird nothwendig irgend eine derselben die ***niedrigste*** sein. Man setze, ihr Exponent sei $=\lambda$. Alsdann ist zunächst zu zeigen, dafs λ ein ***Theiler*** von δ und folglich von $p-1$ sein mufs.

C. Gesetzt λ sei ***nicht*** ein Theiler von δ, also

$$3. \quad \delta = \mathfrak{G}\lambda+\varrho,$$

wo $\varrho > 0$ und $< \lambda$ ist, so müfste, da

$$4. \quad z^\lambda = \mathfrak{G}p+1$$

vorausgesetzt wird, nach (2. und 3.)

$$5. \quad z^\delta = z^{\mathfrak{G}\lambda+\varrho} = z^{\mathfrak{G}\lambda}z^\varrho = \mathfrak{G}p+1,$$

oder, da nach (4.) $z^{\mathfrak{G}\lambda} = (\mathfrak{G}p+1)^{\mathfrak{G}} = \mathfrak{G}p+1$ ist (5.),

$$(\mathfrak{G}p+1)z^\varrho = \mathfrak{G}p+1 \text{ oder}$$

$$6. \quad z^\varrho = \mathfrak{G}p+1$$

sein; also müfste, da $\varrho < \lambda$ ist, eine *noch niedrigere* Potenz als z^λ zu p den Rest 1 lassen. Da dieses gegen die Voraussetzung ist, so kann nicht $\delta = \mathfrak{G}\lambda + \varrho$, sondern nur $\delta = \mathfrak{G}\lambda$ und folglich λ nur ein *Theiler* von δ sein.

D. Nun ist nothwendig jeder Theiler λ von δ ein Theiler von $p-1$ selbst. Und da es nun für *jeden* Theiler λ von $p-1$, so wie für $\lambda = p-1$ selbst, Werthe von z giebt, die der Gleichung $z^\lambda = \mathfrak{G}p+1$ genugthun, so giebt es auch für jeden Theiler λ oder δ von $p-1$ *Stammwurzeln.*

Beweis von II. *E.* Ist δ zu $p-1$ *theilerfremd,* so bekommt nach (§. 56. II.) in

$$7. \quad z^\delta = \mathfrak{G}p+r$$

r für jeden Werth von z einen *andern* Werth und die Werthe von r durchlaufen alle die Zahlen 1, 2, 3, 4, ... $p-1$. Also ist kein r, aufser für $z=1$, gleich 1; mithin findet die Gleichung (1.) nur allein für $z=1$ Statt, und folglich giebt es in diesem Fall *keine* Stammwurzeln.

F. Hat δ mit $p-1$ einen Theiler λ gemein, so dafs z. B.

$$8. \quad \delta = \lambda\eta \text{ und } p-1 = \lambda\tau$$

ist, so giebt es schon für den *kleinsten* Theiler λ von δ Stammwurzeln; denn es giebt deren nach (1.) für *jeden* Exponenten, welcher, wie λ, ein Theiler von $p-1$ ist. Also ist schon

$$9. \quad z^\lambda = \mathfrak{G}p+1,$$

während *zugleich*

$$10. \quad z^\delta = z^{\lambda\eta} = (\mathfrak{G}p+1)^\eta = \mathfrak{G}p+1$$

ist, und die z, welche der Gleichung (10.) oder (1.) entsprechen, sind nicht mehr *Stammwurzeln* aus 1, weil schon die *niedrigere* Potenz z^λ von z den Rest 1 läfst. Mithin giebt es auch in diesem Fall keine *Stammwurzeln* aus 1 zu p, und folglich überhaupt, wenn δ nicht in $p-1$ *aufgeht,* keine δten Stammwurzeln aus 1 zu p; gemäfs (II.).

Anm. *G.* Der Satz geht insbesondere aus (§. 56.) hervor.

§. 59.

Lehrsatz.

Wenn in der Zahlengleichung

$$1. \quad z_\delta^\delta = \mathfrak{G}p+1$$

p *eine Stammzahl,* δ *ein Theiler von* p—1 *und* z_δ *einer der* δ*ten* ***Stammwurzeln*** *aus* 1 *zu* p *ist, so sind*

I. *Die Reste zu allen den Potenzen* $z_\delta^1, z_\delta^2, z_\delta^3, z_\delta^4, \dots z_\delta^\delta$ *von* z *unter einander verschieden, und wenn man die weitern, höheren Potenzen nimmt, so kehren dieselben Reste in derselben Ordnung wieder, und bilden also eine Periode. Das heifst, in Zeichen ausgedrückt: wenn man in der Gleichung*

$$2.\quad z_\delta^{n\delta+\varkappa} = \mathfrak{G}p + r_{n\delta+\varkappa}$$

der Reihe nach

$$3.\quad \varkappa = 1, 2, 3, \dots \delta \text{ und } n = 0, 1, 2, 3, \dots \left(\frac{p-1}{\delta} - 1\right)$$

setzt, so sind die r, *welche sich in* (2.) *ergeben, für ein und dasselbe* n *unter einander verschieden, für gleiche* $\varkappa$ *und verschiedene* n *aber einander gleich, so dafs*

$$4.\quad r_{n\delta+\varkappa} = r_\varkappa.$$

II. *Ist in* (I.) z *eine Hauptstammwurzel, also* $\delta = p-1$, *so durchläuft, wenn man in*

$$5.\quad z_{p-1}^\varkappa = \mathfrak{G}p + r$$

der Reihe nach

$$6.\quad \varkappa = 1, 2, 3, \dots p-1$$

setzt, r *ebenfalls alle die Zahlen* 1, 2, 3, ... p — 1; *nur in anderer Ordnung als* z.

Beispiele. (Aus Taf. I.) Zu I. Für die $\delta = 3$te *Stammwurzel* 13 ist die immerfort wiederkehrende Periode der Reste zu z^1, z^2, z^3 etc. 13, 7 und 1. Für die $\delta = 4$te *Stammwurzel* 50 ist die Periode zu z^1, z^2, z^3, z^4 etc. 50, 60, 11 und 1. Für die $\delta = 10$te *Stammwurzel* 3 ist die Periode der Reste zu $z^1, z^2, z^3, \dots z^{10}$ etc. 3, 9, 27, 20, 60, 58, 52, 34, 41 und 1. U. s. w. Immer sind die Reste in jeder Periode *unter sich verschieden.*

Zu II. Für die *Hauptstammwurzel* 2 z. B. durchlauft r alle die Zahlen 1, 2, 3, 4, ... 60, obwohl in verschiedener Ordnung von $\varkappa$. Eben so verhält sich für die andern *Hauptstammwurzeln* 6, 7, 10, 17 etc.

Beweis *A.* Die Gleichung (2.) ist so viel als

$$7.\quad z^{n\delta} z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa}$$

und, da vermöge (1.) $z^{n\delta} = (\mathfrak{G}p+1)^n = \mathfrak{G}p + 1$ ist, so viel als

$$(\mathfrak{G}p+1) z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa} \text{ oder}$$

$$8.\quad z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa}.$$

Nun ist auch nach (2.)

$$9.\quad z^\varkappa = \mathfrak{G}p + r_\varkappa,$$

also folgt aus (8. und 9.)

$$\mathfrak{S}p + r_{n\delta+\varkappa} = \mathfrak{S}p + r_\varkappa \text{ oder}$$

$$10. \quad r_{n\delta+\varkappa} = \mathfrak{S}p + r_\varkappa$$

und, da beide $r < p$ sein sollen,

$$11. \quad r_{n\delta+\varkappa} = r_\varkappa;$$

gemäfs (4.).

B. Gäben nun z. B.: $z^{\varkappa_1}$ und $z^{\varkappa_2}$ *gleiche* Reste $r_{\varkappa_1} = r_{\varkappa_2}$, so wäre

$$12. \quad z^{\varkappa_1} = \mathfrak{S}p + r_{\varkappa_1} \text{ und } z^{\varkappa_2} = \mathfrak{S}p + r_{\varkappa_2},$$

also

$$13. \quad z^{\varkappa_1} - z^{\varkappa_2} = \mathfrak{S}p,$$

oder, wenn von den beiden Zahlen $\varkappa_1$ und $\varkappa_2$ etwa $\varkappa_1$ die *gröfsere* ist,

$$14. \quad z^{\varkappa_2}(z^{\varkappa_1-\varkappa_2} - 1) = \mathfrak{S}p.$$

Da $z < p$ ist, so geht z und folglich $z^{\varkappa_2}$ mit p *nicht* auf, also müfste, zufolge (14.), $z^{\varkappa_1-\varkappa_2} - 1$ mit p *aufgehen*, mithin

$$15. \quad z^{\varkappa_1-\varkappa_2} = \mathfrak{S}p + 1$$

sein. Aber $\varkappa_1$ und $\varkappa_2$ sind nicht gröfser als δ, wiewohl > 0, also ist $\varkappa_1 - \varkappa_2 < \delta$: folglich gäbe nach (15.) schon eine *niedrigere* Potenz als z^δ zu p den Rest 1. Dies ist der Voraussetzung entgegen, da z eine *Stammwurzel* sein soll. Also können die Potenzen einer *Stammwurzel* z mit Exponenten $< \delta$ nicht *gleiche* Reste r zu p lassen, und folglich sind die Reste zu allen den Potenzen $z^1, z^2, z^3, z^4, \dots z^\delta$ unter einander *verschieden.*

Dieses zusammen ist was (I.) behauptet.

C. Da nach (I.) für *jede Stammwurzel*, also auch für die ***Hauptstammwurzeln***, alle Reste r in (5.) unter sich verschieden sind, wenn man $\varkappa = 1, 2, 3, \dots p-1$ setzt, die ***Anzahl*** der verschiedenen Reste aber so grofs ist, als die der Werthe von $\varkappa$, folglich $= p-1$, und dabei alle $r < p$ sind, so sind die Werthe von r in (5.) nothwendig alle die Zahlen 1, 2, 3, ... $p-1$ selbst. Und zwar sind sie es nothwendig in *anderer* Ordnung als $\varkappa$; denn wenn z. B. für ein *bestimmtes* $\varkappa$, $z^\varkappa = \mathfrak{S}p + r$ ist, so ist *nicht* für $\varkappa+1$, $z^{\varkappa+1} = \mathfrak{S}p + r + 1$, sondern $z^{\varkappa+1}$ oder $z^\varkappa . z = (\mathfrak{S}p + r)z = \mathfrak{S}p + rz$, und rz kann nicht $= r+1$ sein, da alle r für die ***Haupt***stammwurzeln > 1 sind, bis auf das letzte r zu z^{p-1}, also für $\varkappa = p-1$, welches, als das höchste $\varkappa$, das *letzte* ist.

§. 60.

Lehrsatz.

Wenn in der Zahlengleichung

$$1.\quad z_\delta^\varkappa = \mathfrak{G}p + r_\varkappa$$

p *eine Stammzahl,* z_δ *eine δte* ***Stammwurzel*** *aus* 1 *zu* p, *mithin δ ein* ***Theiler*** *von* p—1 *und*

$$2.\quad z_\delta^\delta = \mathfrak{G}p + 1$$

ist, so sind in (1.)

I. *Diejenigen Reste* $r_\varkappa$, *für welche λ der* ***gröfste Gemeintheiler*** *von ϰ und δ ist,* ***alle*** *die* $\frac{\delta}{\lambda}$*ten* ***Stammwurzeln*** *aus* 1 *zu p.*

II. *Diejenigen* $r_\varkappa$ *in* (1.), *für welche ϰ* ***keinen*** *Theiler* >1 *mit δ gemein hat, sind* ***alle*** *die δten* ***Stammwurzeln selbst,*** *also alle die Werthe, welche* z_δ *in* (2.) *haben kann.*

Beispiele. (Aus Taf. I.) Für $\delta = 20$ und z. B. $z = 8$ ist in (1.):

3.	Für $\varkappa =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20,
	$r_\varkappa =$	8	3	24	9	11	27	33	20	38	60	53	38	37	52	50	34	28	41	23	1.

Zu I. Die ϰ, deren gröfster Gemeintheiler mit $\delta = 20$, $\lambda = 2$ ist, sind 2, 6, 14 und 18. Die in (3.) zu diesem ϰ gehörigen *r* sind 3, 27, 52 und 41; und dieses sind die sämmtlichen $\frac{\delta}{\lambda} = 10$ten Stammwurzeln aus 1 zu *p*.

Die ϰ, welche mit $\delta = 20$ zum gröfsten Gemeintheiler $\lambda = 4$ haben, sind 4, 8, 12, 16. Die in (3.) zu diesen ϰ gehörigen *r* sind 9, 20, 58 und 34; und das sind die sämmtlichen $\frac{\delta}{\lambda} = 5$ten Stammwurzeln aus 1 zu *p*.

Die ϰ, welche mit $\delta = 20$ zum gröfsten Gemeintheiler $\lambda = 5$ haben, sind 5 und 15. Die in (3.) zu diesen ϰ gehörigen *r* sind 11 und 50; und dieses sind die sämmtlichen $\frac{\delta}{\lambda} = 4$ten Stammwurzeln aus 1 zu *p*.

Das ϰ, welches mit $\delta = 20$ zum gröfsten Gemeintheiler $\lambda = 10$ hat, ist 10. Das in (3.) zu diesem ϰ gehörige *r* ist 60; und dies ist die einzige $\frac{\delta}{\lambda} = 2$te Stammwurzel aus 1 zu *p*.

Zu II. Die ϰ, welche in (3.) mit δ *keinen* Theiler >1 gemein haben, sind 1, 3, 7, 9, 11, 13, 17 und 19. Die in (3.) zu diesen ϰ gehörigen *r* sind 8, 24, 33, 38, 53, 37, 28 und 23; und dieses sind die sämmtlichen $\delta = 20$ten Stammwurzeln aus 1 zu *p*.

Beweis ***A.*** Man setze

$$4.\quad \delta = \mu\lambda \quad \text{und} \quad \varkappa = \nu\lambda,$$

wo λ den ***gröfsten Gemeintheiler*** von $\varkappa$ und δ bezeichnet. Nimmt man nun in (1.) die $\frac{\delta}{\lambda} = \mu$te Potenz, so ergiebt sich

$$5.\quad z^{\mu\varkappa} = \mathfrak{G}p + r_\varkappa^\mu$$

oder, gemäfs (4.),

$$6.\quad z^{\frac{\delta}{\lambda}\cdot\nu\lambda} = z^{\delta\nu} = \mathfrak{G}p + r_\varkappa^\mu,$$

oder, da nach (1.)

$$7.\quad z^{\nu\delta} = (\mathfrak{G}p+1)^\nu = \mathfrak{G}p+1$$

ist,

$$\mathfrak{G}p+1 = \mathfrak{G}p + r_\varkappa^\mu \text{ oder}$$

$$8.\quad r_\varkappa^\mu = \mathfrak{G}p+1 = r_\varkappa^{\frac{\delta}{\lambda}}.$$

Also läfst die $\mu = \frac{\delta}{\lambda}$te Potenz von $r_\varkappa$ zu p den Rest 1.

B. Aber keine ***niedrigere*** als die $\mu = \frac{\delta}{\lambda}$te Potenz von $r_\varkappa$ kann den Rest 1 lassen; denn wäre es so, so müfste in (8.) λ ein anderer Theiler λ_1 von δ sein, der ***gröfser*** ist als der ***gröfste Gemeintheiler*** λ von δ und $\varkappa$. Ein ***Theiler*** von δ müfste λ_1 ***immer*** sein, weil sonst $\frac{\delta}{\lambda_1}$ keine ***ganze*** Zahl wäre. Es wäre aber für einen solchen Theiler λ_1 in (4.) ν keine ***ganze*** Zahl, da vorausgesetzt ist, dafs λ der ***gröfste*** Gemeintheiler von δ und $\varkappa$ sein soll. Nun könnte zwar $\nu\delta$ in (7.), auch wenn ν ein Bruch ist, immer noch eine ***ganze*** Zahl sein, aber diese Zahl wäre dann kein ***ganzzahliges Vielfache*** von δ, sondern etwa $= n\delta + \varrho$, wo $\varrho > 0$ und $< \delta$ ist. Solche Potenzen von z in (7.) lassen aber zu p ***nicht*** den Rest 1, sondern nach (§. 59. I.) lauter unter einander von 1 ***verschiedene*** Reste. Also kann λ ***nicht gröfser*** sein als der ***gröfste Gemeintheiler*** von δ und $\varkappa$, und folglich läfst in (8.) keine ***kleinere*** als die $\frac{\delta}{\lambda} = \mu$te Potenz von $r_\varkappa$ den Rest 1 zu p, mithin ist $r_\varkappa$ in (8.) eine $\frac{\delta}{\lambda}$te ***Stammwurzel*** aus 1 zu p, und ***jedes*** r, welches die Gleichung (1.) für die verschiedenen Werthe von $\varkappa$ giebt, deren ***gröfster Gemeintheiler*** mit δ gleich λ ist, ist eine ***solche.***

C. Es kann aber auch ***kein anderes*** r als diejenigen, welche die Gleichung (1.) giebt, eine $\frac{\delta}{\lambda}$te Stammwurzel aus 1 zu p sein. Denn die

Gleichung (1.) giebt ***alle r***, für welche δ und $\varkappa$ die Zahl λ zum gröfsten Gemeintheiler hat. ***Andere r*** müfsten also Werthen von $\varkappa$ entsprechen, die mit δ ***andere*** gröfste Gemeintheiler λ_1 hätten, und diese sind dann nach (***B.***) nicht mehr $\frac{\delta}{\lambda}$te, sondern $\frac{\delta}{\lambda_1}$te, also ***andere*** Stammwurzeln aus 1 zu ***p***. Also sind die ***r*** in (1.) ***alle*** $\frac{\delta}{\lambda}$te Stammwurzeln aus 1 zu ***p***, und es giebt ***keine anderen*** weiter.

Dieses zusammen ist was (I.) behauptet.

D. Haben δ und $\varkappa$ in (1.) ***keinen*** Theiler $\lambda > 1$ gemein, so ist ihr ***gröfster Gemeintheiler*** $\lambda = 1$, und folglich in (4.) $\mu = \delta$, also dann in (8.)

$$9.\quad r_\varkappa^\delta = \mathfrak{G}p + 1.$$

Folglich sind dann die $r_\varkappa$ in (1.) alle die δten ***Stammwurzeln z*** aus 1 zu ***p*** selbst; gemäfs (II.).

§. 61.

Lehrsatz.

I. ***Von den verschiedenen δten Stammwurzeln aus 1 zu der Stammzahl*** p ***geben die 1te, 2te, 3te, 4te, ... δte Potenzen gleichmäfsig, obwohl in verschiedener Ordnung, immer dieselben Reste zu*** p, ***unter welchen dann nach*** (§. 60. II.) ***auch die Werthe von*** z ***selbst sind; so dafs also für jede der verschiedenen Stammwurzeln*** z_δ ***in der Gleichung***

$$1.\quad z^\delta = \mathfrak{G}p + 1,$$

wo δ ein Theiler von p—1 ***ist, wenn man in***

$$2.\quad z^\varepsilon = \mathfrak{G}p + r_\varepsilon$$

der Reihe nach

$$3.\quad \varepsilon = 1, 2, 3, 4, \ldots \delta$$

setzt, r_ε ***immer dieselben Zahlen durchlauft, unter denen sich auch die Werthe von*** z ***selbst befinden, jedoch für jeden andern Werth von*** z ***in verschiedener Ordnung.***

II. ***Die Ordnung der Aufeinanderfolge der Reste für irgend eine δte Stammwurzel*** z_2 ***wird durch die Aufeinanderfolge der Reste für eine andere δte Stammwurzel*** z_1 ***dadurch bestimmt, dafs, wenn z. B.***

$$4.\quad z_1^\varkappa = \mathfrak{G}p + z_2$$

ist und man setzt

$$5.\quad z_2^\varepsilon = \mathfrak{G}p + r_\varepsilon,$$

$$6.\quad \varepsilon\varkappa = n\delta + \varkappa_1, \text{ wo } \varkappa_1 < \delta \textit{ und}$$

$$7.\quad z_1^{\varkappa_1} = \mathfrak{S}p + r_{\varkappa_1}:$$

dafs alsdann in (5. *und* 7.)

$$8.\quad r_\varepsilon = r_{\varkappa_1}$$

ist, das heifst, dafs $z_1^{\varepsilon\varkappa}$ *und* z_2^ε *zu* p *gleiche Reste* r_ε *und* $r_{\varkappa_1}$ *lassen, so dafs folglich für je zwei Werthe* z_1 *und* z_2 *von* z_δ, *welche die Gleichung* (4.) *erfüllen,*

$$9.\quad \left\{\begin{matrix} z_1^{\varkappa}, & z_1^{2\varkappa}, & z_1^{3\varkappa}, & z_1^{4\varkappa}, & \dots & z_1^{\delta\varkappa} \\ \textit{und } z_2^1, & z_2^2, & z_2^3, & z_2^4, & \dots & z_2^\delta \end{matrix}\right\} \textit{ zu p gleiche Reste lassen.}$$

Beispiel. (Aus Taf. I.) Zu I. Die $\delta = 10$te Stammwurzeln für $p = 61$ sind nach der Tafel 3, 27, 41, 52, und die 1te, 2te, 3te, 4te, ... 10 ($=\delta$)te Potenzen dieser ***verschiedenen*** Stammwurzeln geben zu p gleichmäfsig ***dieselben*** Reste 3, 9, 27, 20, 60, 58, 52, 34, 41 und 1, unter welchen sich auch die Stammwurzeln 3, 27, 41 und 52 selbst befinden; obwohl in ***verschiedener*** Ordnung.

Zu II. Für die 10te Stammwurzel $z_1 = 3$ giebt z_1^3 zu p den Rest 27, welches ebenfalls eine der 10ten Stammwurzel $z_2 = 27$ ist; also ist für diesen Fall in (4.) $\varkappa = 3$. Nun giebt

$$10.\quad \left\{\begin{array}{llll} z_1^3 & \dots\dots\dots & & \text{den Rest } 27 \text{ zu } p, \\ z_1^6 & \dots\dots\dots & & \text{den Rest } 58 \text{ - -}, \\ z_1^9 & \dots\dots\dots & & \text{den Rest } 41 \text{ - -}, \\ z_1^{12} & \text{oder } z^{1\cdot10+2} & \text{oder } z^2 & \text{den Rest } 9 \text{ - -}, \\ z_1^{15} & \text{oder } z^{1\cdot10+5} & \text{oder } z^5 & \text{- - } 60 \text{ - -}, \\ z_1^{18} & \text{oder } z^{1\cdot10+8} & \text{oder } z^8 & \text{- - } 34 \text{ - -}, \\ z_1^{21} & \text{oder } z^{2\cdot10+1} & \text{oder } z^1 & \text{- - } 3 \text{ - -}, \\ z_1^{24} & \text{oder } z^{2\cdot10+4} & \text{oder } z^4 & \text{- - } 20 \text{ - -}, \\ z_1^{27} & \text{oder } z^{2\cdot10+7} & \text{oder } z^7 & \text{- - } 52 \text{ - -}, \\ z_1^{30} & \text{oder } z^{2\cdot10+10} & \text{oder } z^{10} & \text{- - } 1 \text{ - -}; \end{array}\right.$$

und ***dieselben*** Reste zu p geben z_2^1, z_2^2, z_2^3, z_2^4, z_2^5, z_2^6, z_2^7, z_2^8, z_2^9 und z_2^{10}; gemäfs (9.).

Beweis ***A.*** Für jedes ε in (2.), welches mit δ keinen Theiler >1 gemein hat, ist nach (§. 60 II.) r_ε eine δte ***Stammwurzel*** aus 1 zu p. Alle diejenigen $\varkappa$ also, welche zu δ ***theilerfremd*** sind, erfüllen die Gleichung (4.).

B. Nimmt man nun von (4.) die Potenz ε, so ergiebt sich

$$11.\quad z_1^{\varepsilon\varkappa} = \mathfrak{S}p + z_2^\varepsilon$$

oder, nach (6.) ausgedrückt,

$$z_1^{n\delta+\varkappa_1} = \mathfrak{G}p + z_2^\varepsilon \text{ oder}$$

$$12.\quad z_1^{n\delta} z_1^{\varkappa_1} = \mathfrak{G}p + z_2^\varepsilon,$$

oder, da aus (1.)

$$13.\quad z_1^{n\delta} = (\mathfrak{G}p+1)^n = \mathfrak{G}p+1$$

ist,

$$(\mathfrak{G}p+1) z_1^{\varkappa_1} = \mathfrak{G}p + z_2^\varepsilon \text{ oder}$$

$$14.\quad z_2^\varepsilon = \mathfrak{G}p + z_1^{\varkappa_1}.$$

C. Läfst man nun in (6.) ε der Reihe nach alle die Zahlen 1, 2, 3, 4, ... δ durchlaufen, so durchlauft nach (§. 34. I.), da $\varkappa$ und δ nach der Voraussetzung zu einander theilerfremd sind, $\varkappa_1$ in (6.) ebenfalls *alle diese Zahlen,* obwohl in verschiedener Ordnung. Setzt man also in (14.) nach (5. und 6.)

$$15.\quad z_2^\varepsilon = \mathfrak{G}p + r_\varepsilon \text{ und}$$

$$16.\quad z_1^{\varkappa_1} = \mathfrak{G}p + r_{\varkappa_1}$$

und läfst in (15.) ε alle die Zahlen 1, 2, 3, 4, ... δ durchlaufen, so durchlauft $\varkappa_1$ nach (6.) ebenfalls *alle* diese Zahlen, und folglich durchlauft auch, vermöge (14.), $r_{\varkappa_1}$ in (16.) *alle dieselben* Zahlen wie r_ε in (15.), indem nach (14.) z_2^ε und $z_1^{\varkappa_1}$ nur um Vielfache von p verschieden sind und sie also *dieselben* Reste r_ε und $r_{\varkappa_1}$ zu p geben müssen. Folglich durchlauft r_ε in (2.), wenn man der Reihe nach $\varepsilon = 1, 2, 3, 4, \ldots . \delta$ setzt, für *jedes* z_2 oder z_1, welches eine δte *Stammwurzel* aus 1 zu p ist, immer *dieselben* Zahlen. Dieses ist was (I.) behauptet.

D. Setzt man (15. und 16.) in (14.), so ergiebt sich

$$\mathfrak{G}p + r_\varepsilon = \mathfrak{G}p + \mathfrak{G}p + r_{\varkappa_1}, \text{ oder}$$

$$17.\quad r_\varepsilon = \mathfrak{G}p + r_{\varkappa_1}$$

und, da r_ε und $r_{\varkappa_1}$ beide $< p$ sind,

$$18.\quad r_\varepsilon = r_{\varkappa_1};$$

gemäfs (II. 8.).

E. Anm. Die gegenwärtigen Sätze gehen aus (§. 34. und 40.) hervor

§. 62.

Lehrsatz.

Wenn in der Zahlengleichung

$$1.\quad \mathrm{x}^\delta = \mathfrak{G}\mathrm{p} + \mathrm{r}$$

p ***eine Stammzahl,*** δ ***ein Theiler von*** $\mathrm{p}-1$ ***ist, und*** z ***ist in***

$$2.\quad \mathrm{z}^\delta = \mathfrak{G}\mathrm{p} + 1$$

irgend eine δ***te Stammwurzel aus*** 1 ***zu*** p, ***und man setzt***

3. $z^{\varkappa} = \mathfrak{S}p + r_1$,

4. $r_1 x = \mathfrak{S}p + y$ und

5. $y^{\delta} = \mathfrak{S}p + \varrho$,

so ist in (1. *und* 5.)

6. $r = \varrho$

für jede δ*te Stammwurzel* z *aus* 1 *zu* p *und für jeden Werth von* $\varkappa > 0$ *und* $< \delta + 1$.

Oder in Worten: Die δ***te Potenz einer beliebigen Zahl*** x ***giebt, wenn*** δ ***ein Theiler von*** $p-1$ ***ist, zu*** p ***denselben Rest*** r, ***wie die*** δ***ten Potenzen von*** xz, xz^2, xz^3, xz^4, ... xz^{δ} ***für jede*** δ***te Stammwurzel*** z ***aus*** 1 ***zu*** p. ***Auch giebt die*** δ***te Potenz keiner andern Zahlen den Rest*** r.

Beispiel. (Aus Taf. I.) Es sei

7. $x = 12$, $\delta = 6$.

Zu $\delta = 6$ ist

8. $z = 14$

eine Stammwurzel. Für diese ist in (3.), wenn man $\varkappa$ der Reihe nach $= 1$, 2, 3, 4, 5 und 6 setzt,

9. $r_1 = 14, 13, 60, 47, 48$ und 1,

und in (4.) ist $14.12 = 168 = 2.p + 46$, $13.12 = 156 = 2.p + 34$, $60.12 = 720 = 8.p + 49$, $47.12 = 564 = 9.p + 15$, $48.12 = 576 = 9.p + 27$ und $1.12 = 0.p + 12$, also

10. $y = 46, 34, 49, 15, 27$ und 12.

Endlich ist für (5.), wie es sich aus der Tafel entnehmen läfst, wenn man 46, 34, 49, 15, 27 und 12 in der *obersten* horizontalen Reihe aufsucht und die zugehörigen Zahlen in der *sechsten* horizontalen Zeile nimmt,

11. $46^6 = \mathfrak{S}p + 34$, $34^6 = \mathfrak{S}p + 34$, $49^6 = \mathfrak{S}p + 34$, $15^6 = \mathfrak{S}p + 34$, $27^6 = \mathfrak{S}p + 34$ und $12^6 = \mathfrak{S}p + 34$.

Also sind für (5.) alle $\varrho = 34$ und $= r$.

Beweis. *A.* In (1.) x mit $z^{\varkappa}$ multiplicirt, giebt $(xz^{\varkappa})^{\delta} = x^{\delta} z^{\varkappa\delta}$. Aber $z^{\delta} = \mathfrak{S}p + 1$ (2.), also $z^{\varkappa\delta} = (\mathfrak{S}p + 1)^{\varkappa} = \mathfrak{S}p + 1$ und folglich

12. $(xz^{\varkappa})^{\delta} = (\mathfrak{S}p + 1)x^{\delta} = \mathfrak{S}p + x^{\delta} = \mathfrak{S}p + \mathfrak{S}p + r$ (1.) $= \mathfrak{S}p + r$;

also giebt x, multiplicirt mit *jeder* Potenz $z^{\varkappa}$ von z, die δte Potenz *derselben* Reste r, wie die δte Potenz von x selbst.

B. Zu jedem *Theiler* δ von $p-1$ gehören zu *demselben* r *nur* δ verschiedene Werthe von x (§. 54. I.). Die Multiplication von x mit z^1, z^2,

z^3, ... z^δ giebt δ Zahlen, die, zur Potenz δ erhoben, ***denselben*** Rest r lassen, und alle diese Zahlen sind ***verschieden:*** denn zu z^1, z^2, z^3, ... z^δ sind in (3.), da z die δte *Stammwurzel* aus 1 zu p sein soll, alle die Reste r_1 ***verschieden,*** also auch alle die y in (4.), und alle die ϱ in (5.); mithin giebt die Multiplication von x mit z^1, z^2, z^3, ... z^δ ***alle*** die δ Zahlen, von welchen die Potenz δ zu p ***denselben*** Rest r läfst; und es giebt keinen andern.

Dies zusammen ist, was der Lehrsatz in ***Worten*** behauptet.

C. Dafs das, was der Lehrsatz in ***Zeichen*** ausspricht, das Nemliche ist, ergiebt sich wie folgt. Es ist

13. $$(xz^\varkappa)^\delta = (x(\mathfrak{G}p + r_1))^\delta \; (3.) = \mathfrak{G}p + (r_1 x)^\delta = \mathfrak{G}p + (\mathfrak{G}p + y)^\delta \; (4.)$$
$$= \mathfrak{G}p + y^\delta = \mathfrak{G}p + \varrho \; (5.).$$

Aber

14. $$x^\delta = \mathfrak{G}p + r,$$

und da $(xz^\varkappa)^\delta$ und x^δ, wie sich fand, zu p ***gleiche*** Reste lassen, so ist

15. $$r = \varrho;$$

gemäfs (6.).

Anm. ***D.*** Der Satz beruht insbesondere auf (§. 54.).

§. 63.

Lehrsatz.

I. ***Die Anzahl der Stammwurzeln*** z_δ ***aus*** 1 ***zu einer Stammzahl*** p, ***für jeden beliebigen Exponenten*** δ, ***der nach*** (§. 58.) ***in*** p — 1 ***aufgehen mufs, also auch für den Exponenten*** p — 1 ***selbst, ist der Anzahl der Zahlen*** >0 ***und*** $<\delta$ ***gleich, die mit*** δ ***keinen Theiler*** >1 ***gemein haben.***

II. ***Zu jedem andern in*** p — 1 ***aufgehenden Exponenten gehören andere Stammwurzeln aus*** 1 ***zu*** p.

III. ***Die Stammwurzeln*** z_δ ***aus*** 1 ***zu*** p, ***mit allen den verschiedenen Theilern*** δ ***von*** p — 1, ***also auch mit*** p — 1 ***selbst zu Exponenten, sind zusammen alle die Zahlen*** 1, 2, 3, 4, ... p — 1.

IV. ***Wenn man eine der Hauptstammwurzeln*** z_{p-1} ***kennt, so geben die Reste ihrer verschiedenen Potenzen zu*** p, ***von der*** 1***ten an, bis zur*** p — 1***ten, nicht allein die übrigen Hauptstammwurzeln, sondern auch die sämmtlichen Stammwurzeln für alle in*** p — 1 ***aufgehende Exponenten. Die Hauptstammwurzeln*** z_{p-1} ***aus*** 1 ***zu*** p ***sind, wenn*** z_{p-1} ***eine derselben ist, in***

1. $$z_{p-1}^\varkappa = \mathfrak{G}p + r_\varkappa$$

diejenigen $r_\varkappa$, *deren Zeiger* $\varkappa$ *mit* $p-1$ ***keinen Theiler*** >1 ***gemein haben.*** *Die Stammwurzeln* z_δ *dagegen aus* 1 *zu* p, *für einen* ***beliebigen in*** $p-1$ ***aufgehenden Exponenten*** δ, *sind die* $r_\varkappa$, *deren Zeiger* $\varkappa$ *mit* $p-1$ *zum* ***gröfsten*** *Gemeintheiler* $\frac{p-1}{\delta}$ *haben; so dafs man also vermittels* ***einer*** *der* ***Hauptstammwurzeln alle Stamm- und Hauptstammwurzeln*** *unmittelbar unter den Potenzenresten jener* ***einen*** *Hauptstammwurzel findet.*

Beispiele. (Aus Taf. I.) Was der Lehrsatz behauptet, wird sich zusammengenommen in dem Beispiel $p=61$ in folgender Übersicht zeigen.

2. Es sind die ***Hauptstammwurzeln***
$z_{p-1} = 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55$ und 59,
z. B. für $z_{p-1}=2$ in (1.) die Reste $r_\varkappa$ für
$\varkappa = 1, 7, 49, 23, 47, 13, 41, 29, 59, 11, 43, 17, 53, 19, 37$ und 31;
für $z_{p-1}=6$ in (1.) die Reste $r_\varkappa$ für
$\varkappa = 43, 1, 7, 29, 41, 19, 23, 47, 17, 53, 49, 11, 59, 37, 31$ und 13;
für $z_{p-1}=7$ in (1.) die Reste $r_\varkappa$ für
$\varkappa = 49, 43, 1, 47, 23, 37, 29, 41, 11, 59, 7, 53, 17, 31, 13$ und 19.
. .

3. Es sind die $\delta=30$ten Stammwurzeln $z_{30} = 4, 5, 19, 36, 39, 45, 46, 49$,
z. B. für $z_{p-1}=2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 2, 22, 26, 14, 46, 34, 58, 38$;
für $z_{p-1}=6$ - - - - $r_\varkappa$ - $\varkappa = 26, 46, 38, 2, 58, 22, 34, 14$;
für $z_{p-1}=7$ - - - - $r_\varkappa$ - $\varkappa = 38, 58, 14, 26, 34, 46, 22, 2$.
. .

4. Es sind die $\delta=20$ten Stammwurzeln $z_{20} = 8, 23, 24, 28, 33, 37, 38, 53$,
z. B. für $z_{p-1}=2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 3, 57, 9, 51, 21, 39, 27, 33$;
für $z_{p-1}=6$ - - - - $r_\varkappa$ - $\varkappa = 9, 51, 27, 33, 3, 57, 21, 39$;
für $z_{p-1}=7$ - - - - $r_\varkappa$ - $\varkappa = 27, 33, 21, 39, 9, 51, 3, 57$.
. .

5. Es sind die $\delta=15$ten Stammwurzeln $z_{15} = 12, 15, 16, 22, 25, 42, 56, 57$,
z. B. für $z_{p-1}=2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 8, 28, 4, 16, 44, 56, 52, 32$;
für $z_{p-1}=6$ - - - - $r_\varkappa$ - $\varkappa = 44, 4, 52, 28, 32, 8, 16, 56$;
für $z_{p-1}=7$ - - - - $r_\varkappa$ - $\varkappa = 32, 52, 16, 4, 56, 44, 28, 8$.
. .

Es sind die $\delta = 12$ten Stammwurzeln $z_{12} = 21, 29, 32, 40,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 55, 35, 5, 25;$
6. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 25, 5, 35, 55;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 55, 35, 5, 25.$
. .

Es sind die $\delta = 10$ten Stammwurzeln $z_{10} = 3, 27, 41, 52,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 6, 18, 54, 42;$
7. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 18, 54, 42, 6;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 54, 42, 6, 18.$
. .

Es sind die $\delta = 6$ten Stammwurzeln $z_6 = 14, 48,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 50, 10;$
8. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 50, 10;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 50, 10.$
.

Es sind die $\delta = 5$ten Stammwurzeln $z_5 = 9, 20, 34, 58,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 12, 24, 48, 36;$
9. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 36, 12, 24, 48;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 48, 36, 12, 24.$
. .

Es sind die $\delta = 4$ten Stammwurzeln $z_4 = 11, 50,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 15, 45;$
10. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 45, 15;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 15, 45.$
.

Es sind die $\delta = 3$ten Stammwurzeln $z_3 = 13, 47,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste $r_\varkappa$ für $\varkappa = 40, 20;$
11. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 40, 20;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 40, 20.$
.

Es ist die $\delta = 2$te Stammwurzel $z_2 = 60,$
z. B. für $z_{p-1} = 2$ in (1.) der Rest $r_\varkappa$ für $\varkappa = 30;$
12. für $z_{p-1} = 6$ - - - - $r_\varkappa$ - $\varkappa = 30;$
für $z_{p-1} = 7$ - - - - $r_\varkappa$ - $\varkappa = 30.$
.

13. $\left\{ \begin{array}{l} \text{Es ist die } \delta = 1\text{te Stammwurzel } z_1 = 1 \\ \text{für alle } z_{p-1} \text{ in (1.) der Rest } r_x \text{ für } x = 60. \end{array} \right.$

Hier sind nun, wie man sieht,

a. In (2.) die Werthe von x für die verschiedenen ***Hauptstammwurzeln*** z_{p-1} ***dieselben;*** wie es sein mufs, da *jede* Hauptstammwurzel das *Nemliche* giebt.

b. In (2.), für die Hauptstammwurzeln $z_{p-1} = z_{60}$, sind die Werthe 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 und 59 von x alle die Zahlen, welche mit $p - 1 = 60$ keinen Theiler > 1 gemein haben.

In (3.), für die Stammwurzeln $z_\delta = z_{30}$, sind die Werthe 2, 14, 22, 26, 34, 38, 46 und 58 von x alle die Zahlen, welche mit $p - 1 = 60$, $\frac{p-1}{\delta} = \frac{60}{30} = 2$ zum ***gröſsten Gemeintheiler*** haben.

In (4.), für die Stammwurzeln $z_\delta = z_{20}$, sind die Werthe 3, 9, 21, 27, 33, 39, 51 und 57 von x alle die Zahlen, welche mit $p - 1 = 60$, $\frac{p-1}{\delta} = \frac{60}{20} = 3$ zum ***gröſsten Gemeintheiler*** haben.

Und so weiter in (5. 6. 7. 13.) für $\delta = 15, 12, 10, 6, 5, 4, 3, 2$ und 1; wie es gemäfs (IV.) sein soll.

c. Die *Anzahl* der verschiedenen Stammwurzeln ist jedesmal der Anzahl der Zahlen gleich, welche mit δ keinen Theiler > 1 gemein haben; gemäfs (I.). Nemlich:

Zu $\delta = p - 1 = 60$ giebt es gemäfs (2.) 16 Stammwurzeln,
und die 16 Zahlen 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 und 59 haben mit $\delta = 60$ keinen Theiler > 1 gemein.

Zu $\delta = 30$ giebt es gemäfs (3.) 8 Stammwurzeln,
und die 8 Zahlen 1, 7, 11, 13, 17, 19, 23 und 29 haben mit $\delta = 30$ keinen Theiler > 1 gemein.

Für $\delta = 20$ giebt es gemäfs (3.) 8 Stammwurzeln,
und die 8 Zahlen 1, 3, 7, 9, 11, 13, 17 und 19 haben mit $\delta = 20$ keinen Theiler > 1 gemein.

Und so weiter.

d. Zu jedem Exponenten δ gehören, wie (2. 3. 13.) zeigen, ***andere*** Stammwurzeln z_δ; gemäfs (II.).

e. Alle Stammwurzeln in (2. 3. 13.) sind zusammen ***alle*** die Zahlen 1, 2, 3, 4, ... 60; gemäfs (III.).

Beweis. *A.* Der Beweis von (IV.) liegt unmittelbar in (§. 60. I. und II.) und ist daselbst ausgesprochen.

B. Nach (§. 60. I.) sind in

$$14.\quad z^{\varkappa}_{\delta} = \mathfrak{G}p + r_{\varkappa}$$

diejenigen $r_{\varkappa}$, für welche der *gröfste Gemeintheiler* von $\varkappa$ und δ, λ ist *alle* die $\frac{\delta}{\lambda} = \delta_1$ten Stammwurzeln aus 1 zu p.

a. Setzt man

$$15.\quad \varkappa = 1, 2, 3, 4, \ldots \delta,$$

so haben von diesen δ Zahlen

$$16.\quad \text{die } \frac{\delta}{\lambda} = \delta_1 \text{ Zahlen } \lambda,\ 2\lambda,\ 3\lambda,\ 4\lambda,\ \ldots \frac{\lambda}{\delta}.\lambda,$$

und *keine andern,* mit δ den Theiler λ gemein. Nur diese $\frac{\delta}{\lambda} = \delta_1$ Zahlen unter denen (15.) kommen für die Werthe von $\varkappa$, welche in (14.) durch die r die $\frac{\delta}{\lambda} = \delta_1$ten Stammwurzeln geben, in Betracht; denn alle diese $\varkappa$ *sollen* mit λ *aufgehen.* Aber *unter* den δ_1 Zahlen (16.) befinden sich auch *alle* $\varkappa$, auf welche es ankommt.

b. Es sollen aber von den δ_1 Zahlen (16.), *unter welchen* sich die gesuchten $\varkappa$ befinden, nur *diejenigen* genommen werden, welche mit

$$17.\quad \delta = \delta_1 \lambda \ (16.)$$

keinen gröfsern Theiler als λ gemein haben. Diese sind die *gesuchten* $\varkappa$. Drückt man die δ_1 Zahlen (16.) allgemein durch

$$18.\quad \varepsilon = \tau\lambda$$

aus, wo nun $\tau = 1, 2, 3, 4, \ldots \delta_1 \left(= \frac{\delta}{\lambda}\right)$ ist, so sind jene *gesuchten* $\varkappa$, welche mit δ *keinen gröfsern* Theiler als $\varkappa$ gemein haben, offenbar diejenigen, und nur diejenigen ε, für welche τ in (18.) mit δ_1 in (17.) *keinen Theiler* > 1 gemein hat: denn so wie τ noch irgend einen Theiler $\mu > 1$ von δ mit δ_1 gemein hat, so ist der *gröfste* Gemeintheiler von ε und δ nicht mehr λ, sondern $\mu\lambda > \lambda$.

c. Es folgt also, dafs die *Anzahl* derjenigen $\varkappa$, deren *gröfster Gemeintheiler* mit δ, λ ist, *dieselbe* sein mufs, wie die Anzahl der Zahlen, welche mit $\delta_1 = \frac{\delta}{\lambda}$ *keinen Theiler* > 1 gemein haben, oder welche zu δ_1 *theilerfremd* sind.

d. Diese z nun geben *alle* die $\delta_1 = \frac{\delta}{\lambda}$ten Stammwurzeln: also ist die *Anzahl* dieser $\frac{\delta}{\lambda}$ten Stammwurzeln der Anzahl der zu $\delta_1 = \frac{\delta}{\lambda}$ *theilerfremden* Zahlen gleich. Folglich ist allgemein, δ statt δ_1 gesetzt, die Anzahl der Stammwurzeln aus 1 zu p für einen beliebigen Exponenten δ, welcher in $p-1$ *aufgeht*, der Anzahl der Zahlen >0 und $<\delta$ gleich, die mit δ keinen Theiler >1 gemein haben; gemäfs (I.).

C. Gehörte eine und dieselbe Stammwurzel z zu zwei verschiedenen in $p-1$ aufgehenden Exponenten δ_1 und δ_2, so müfste

$$19. \quad z^{\delta_1} = \mathfrak{G}p+1 \text{ und zugleich}$$

$$20. \quad z^{\delta_2} = \mathfrak{G}p+1$$

sein. Dies ist nicht der Fall; denn wenn z. B. von den beiden Exponenten δ_1 und δ_2 der letztere der *gröfsere* ist, so giebt nicht z^{δ_1} den Rest 1 zu p, sondern einen Rest >1, indem *alle* Potenzen $z^1, z^2, z^3, \ldots z^{\delta_2}$, und also auch z^{δ_1} *andere* Reste als 1 geben und *zuerst* die Potenz z^{δ_2} den Rest 1 giebt. So will es die Bedingung, dafs z eine δ_2te *Stammwurzel* sei. Also gehören zu jedem in $p-1$ aufgehenden Exponenten δ *andere* Stammwurzeln aus 1 zu p; gemäfs (II.).

D. *Jede* der Zahlen $1, 2, 3, 4, \ldots p-1$ giebt, zu irgend einer Potenz erhoben, deren Exponent δ entweder $p-1$ selbst, oder ein *Theiler* von $p-1$ ist, nachdem $z^1, z^2, z^3, \ldots z^{\delta-1}$ andere Reste gegeben haben, zu z^δ den Rest 1 (§. 58.). *Jede* der Zahlen $1, 2, 3, \ldots p-1$ ist also nothwendig irgend eine *Stammwurzel*. Ihre Potenzen erreichen immer, entweder schon mit irgend einem Theiler δ von $p-1$, oder mit $p-1$ selbst zum Exponenten, *jedenfalls* den Rest 1. Aber zu jedem Exponenten δ gehören *andere* Stammwurzeln (II.): also kommt jede der Zahlen als Stammwurzel *nur einmal* vor; *alle* aber kommen als solche vor. Also sind die verschiedenen möglichen Stammwurzeln alle die Zahlen $1, 2, 3, 4, \ldots p-1$; gemäfs (III.).

Anm. *E.* Die gegenwärtigen Sätze gehen aus (§. 58. und 60.) hervor, mit Hülfe der Erwägungen in (*B.*).

§. 64.

Lehrsatz.

I. *Wenn* p *eine Stammzahl ist,* δ *und* μ *beliebige Zahlen sind, und man setzt in*

$$1. \quad z^\delta = \mathfrak{G}p+r \text{ und}$$

$$2. \quad z^{\mu\delta} = \mathfrak{G}p+\varrho$$

der Reihe nach

$$3. \quad z = 1, 2, 3, 4, \ldots\ p-1,$$

so sind alle die Werthe von ϱ *in* (2.) *unter den Werthen von* r *in* (1.) *mitbegriffen.*

II. *Wenn* $\lambda_1, \lambda_2, \lambda_3, \ldots$ *die in* $p-1$ *aufgehenden Stammzahlen sind, und* $\delta\lambda_1, \delta\lambda_2, \delta\lambda_3, \ldots$ *gehen ebenfalls noch in* $p-1$ *auf, also auch* δ, *so erhält man, wenn man von den Werthen, welche* r *in* (1.) *für* $z = 1, 2, 3, 4, \ldots\ p-1$ *bekommt, die Werthe ausschliefst, welche in*

$$4. \quad z^{\delta\lambda_1} = \mathfrak{G}p + \varrho_1, \quad z^{\delta\lambda_2} = \mathfrak{G}p + \varrho_2, \quad z^{\delta\lambda_3} = \mathfrak{G}p + \varrho_3, \ldots$$

die Reste $\varrho_1, \varrho_2, \varrho_3, \ldots$, *ebenfalls für* $z = 1, 2, 3, 4, \ldots\ p-1$ *annehmen und welche nach* (I.) *unter den Werthen von* r *in* (1.) *mitbegriffen sind, die* $\frac{p-1}{\delta}$*ten Stammwurzeln aus* 1 *zu* p.

III. *Für* $\delta = 1$ *erhält man also die Hauptstammwurzeln, wenn man von den Zahlen* $1, 2, 3, 4, \ldots\ p-1$ *selbst die Reste zu denjenigen ihrer Potenzen ausschliefst, deren Exponenten* $\lambda_1, \lambda_2, \lambda_3, \ldots$ *die in* $p-1$ *aufgehenden Stammzahlen sind.*

IV. *Auch erhält man die* $\frac{p-1}{\delta}$*ten Stammwurzeln aus* 1 *zu* p, *wenn man von den Werthen von* r *in* (1.) *diejenigen ausschliefst, für welche, wenn* $\varkappa$ *die sämmtlichen Theiler von* $\frac{p-1}{\delta}$ *bezeichnet, in*

$$5. \quad r^{\varkappa} = \mathfrak{G}p + R,$$

$R = 1$ *ist.*

Anm. Will man die $\frac{p-1}{\delta}$ten Stammwurzeln *nach* (II.) berechnen, so mufs man zunächst alle r in (1.) suchen. Sie ergeben sich schon, wenn man $z = 1, 2, 3, 4, \ldots\ \frac{1}{2}(p-1)$ setzt; denn für die *übrigen* z sind nach (§. 54. V.) die r entweder *dieselben*, zu $p-z$, oder sie ergeben sich aus jenen, wenn man sie von p *abzieht.* In (4.) sind dann ebenfalls den z alle die Werthe $1, 2, 3, 4, \ldots\ \frac{1}{2}(p-1)$ beizulegen, aber *nur* für die Exponenten $\delta\lambda_1, \delta\lambda_2, \delta\lambda_3, \ldots$

Will man dagegen die $\frac{p-1}{\delta}$ten Stammwurzeln *nach* (IV.) berechnen, so sind, nachdem, wie vorhin, die r in (1.) gefunden worden sind, den r in (5.) *nur alle die gefundenen Werthe von* r beizulegen nöthig: aber für *alle* die verschiedenen Exponenten $\varkappa$, welche in $\frac{p-1}{\delta}$ aufgehen.

Beispiele. (Aus Taf. I.) Zu I. In (1. und 2.) ist, der Tafel gemäfs, z. B.

6. Für $\delta = 6$, $r = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60$,
- $\mu\delta = 12$, $\varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots$,
- $\mu\delta = 18$, $\varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60$,
- $\mu\delta = 24$, $\varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots$,
- $\mu\delta = 30$, $\varrho = 1 \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots 60$,
- $\mu\delta = 36$, $\varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots$,
- $\mu\delta = 42$, $\varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60$,
- $\mu\delta = 48$, $\varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots$,
- $\mu\delta = 54$, $\varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60$.

Immer sind die ϱ in (2.), wie man sieht, unter den r *mitbegriffen.*

Ist δ zu $p-1$ *theilerfremd,* so sind nach (§. 55. II.) die r in (1.) alle die Zahlen $1, 2, 3, 4, \ldots, p-1$; also sind auch dann in (2.) die ϱ unter den r in (1.) *mitbegriffen;* gemäfs (I.).

Zu II. Die in $p-1=60$ aufgehenden *Stammzahlen* $\lambda_1, \lambda_2, \lambda_3, \ldots$ sind 2, 3 und 5. $\delta=4$ ist einer der Theiler von $p-1$, und von den Exponenten $\delta\lambda_1=8$, $\delta\lambda_2=12$ und $\delta\lambda_3=20$, für (4.), gehen $\delta\lambda_2=12$ und $\delta\lambda_3=20$ in $p-1$ auf. Nun ist in (1. und. 4.) nach der Tafel:

7. Für $\delta = 4$, $r = 1\ 9\ 12\ 13\ 15\ 16\ 20\ 22\ 25\ 34\ 42\ 47\ 56\ 57\ 58$,
- $\delta\lambda_2 = 12$, $\varrho_2 = 1\ 9 \ldots \ldots \ldots \ldots 20 \ldots \ldots 34 \ldots \ldots \ldots \ldots 58$,
- $\delta\lambda_3 = 20$, $\varrho_3 = 1 \ldots \ldots 13 \ldots \ldots \ldots \ldots \ldots \ldots \ldots 47 \ldots \ldots \ldots$

Schliefst man die ϱ_2 und ϱ_3 von den r aus, so bleiben 12, 15, 16, 22, 25, 42, 56 und 57 übrig, und diese Zahlen sind, wie die Tafel zeigt, die $\frac{p-1}{\delta} = \frac{60}{4} = 15$ten *Stammwurzeln* aus 1 zu p; gemäfs (II.).

Zu III. Für die *Stammzahlen* $\lambda_1=2$, $\lambda_2=3$ und $\lambda_3=5$, welche in $p-1=60$ aufgehen, und für $\delta=1$, ist in (4.), der Tafel zufolge:

8. Für $\lambda_1=2$, $\varrho_1 = 1\,3\,4\,5 \ldots 9 \ldots 12\,13\,14\,15\,16\,19\,20 \ldots 22 \ldots \ldots 25\,27 \ldots \ldots \ldots \ldots 34\,36 \ldots \ldots 39 \ldots 41\,42\,45\,46\,47\,48\,49 \ldots 52 \ldots 56\,57\,58\,60$,
Für $\lambda_2=3$, $\varrho_2 = 1\,3 \ldots 8\,9\,11 \ldots \ldots \ldots \ldots \ldots \ldots 20 \ldots \ldots 23\,24 \ldots 27\,28 \ldots \ldots 33\,34 \ldots 37\,38 \ldots \ldots 41 \ldots \ldots \ldots \ldots \ldots \ldots 50\,52\,53 \ldots \ldots 58\,60$,
Für $\lambda_3=5$, $\varrho_3 = 1 \ldots \ldots \ldots 11 \ldots 13\,14 \ldots \ldots \ldots \ldots 21 \ldots \ldots \ldots \ldots \ldots \ldots 29\,32 \ldots \ldots \ldots \ldots \ldots \ldots 40 \ldots \ldots \ldots \ldots 47\,48 \ldots 50 \ldots \ldots \ldots \ldots \ldots 60$.

Schliefst man diese verschiedenen Zahlen $\varrho_1, \varrho_2, \varrho_3$ von den Zahlen 1, 2, 3, 4, ... 60 aus, so bleiben die Zahlen 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55 und 59 übrig, und diese sind die ***Hauptstammwurzeln*** aus 1 zu p; gemäfs (III.).

Zu IV. Für $\delta=5$ z. B. ist $\frac{p-1}{\delta} = \frac{60}{5} = 12$. Die Theiler von 12 sind 2, 3, 4 und 6, also ist in (5.) $\varkappa = 2, 3, 4$ und 6. Nun ist für (1. u. 5.) nach der Tafel:

$$9.\quad \left\{\begin{array}{lllllllllllll}
\text{Für } \delta = 5, & r = 1 & 11 & 13 & 14 & 21 & 29 & 32 & 40 & 47 & 48 & 50 & 60; \\
\text{Für } \varkappa = 2, & R = 1 & 60 & 47 & 13 & 14 & 56 & 48 & 14 & 13 & 47 & 60 & 1, \\
\text{ - } \varkappa = 3, & R = 1 & 50 & 1 & 60 & 50 & 27 & 11 & 11 & 1 & 60 & 11 & 60, \\
\text{ - } \varkappa = 4, & R = 1 & 1 & 13 & 47 & 10 & 25 & 47 & 13 & 47 & 13 & 1 & 1, \\
\text{ - } \varkappa = 6, & R = 1 & 60 & 1 & 1 & 60 & 48 & 60 & 60 & 1 & 1 & 60 & 1.
\end{array}\right.$$

Die Werthe 1, 11, 13, 14, 47, 48 und 60 geben für ein oder das andere $\varkappa$ in (5.) den Rest $R = 1$. Sie müssen also von den Werthen von r in der obersten Zeile (9.) ausgeschlossen werden. Die übrig bleibenden r sind 21, 29, 32 und 40, und diese sind, wie die Tafel zeigt, die $\frac{p-1}{\delta} = 12$ten Stammwurzeln aus 1 zu p; gemäſs (IV.).

Beweis. Von I. *A*. Setzt man, für irgend ein bestimmtes r,

$$10.\quad r^{\mu} = \mathfrak{G}p + k,$$

so ist jedenfalls k ***irgend eine*** der Zahlen $z = 1, 2, 3, 4, \ldots p-1$. Nun giebt die δte Potenz von (10.)

$$11.\quad r^{\mu\delta} = \mathfrak{G}p + k^{\delta}.$$

Aber da die δten Potenzen *aller* der Zahlen $1, 2, 3, \ldots p-1$ in (1.) nur die Reste r geben, so kann auch die δte Potenz von k nur ***eins der*** r geben, z. B. r_1; folglich ist

$$12.\quad k^{\delta} = \mathfrak{G}p + r_1,$$

mithin in (11.)

$$13.\quad r^{\mu\delta} = \mathfrak{G}p + \mathfrak{G}p + r_1 = \mathfrak{G}p + r_1.$$

Zufolge (2.) ist aber

$$14.\quad r^{\mu\delta} = \mathfrak{G}p + \varrho,$$

also ist aus (13. und 14.) $\mathfrak{G}p + r_1 = \mathfrak{G}p + \varrho$ oder

$$15.\quad \varrho = \mathfrak{G}p + r_1$$

und, da r_1 und ϱ beide $< p$ sind,

$$16.\quad \varrho = r_1;$$

mithin ist ϱ irgend einem r gleich, und folglich sind *alle* Werthe von ϱ in (1.) ***mitbegriffen.***

Beweis von II. *B*. Für *alle* r in (1.) ist

$$17.\quad r^{\frac{p-1}{\delta}} = \mathfrak{G}p + 1,$$

denn die $\frac{p-1}{\delta}$te Potenz von (1.) giebt

$$18.\quad z^{\delta\cdot\frac{p-1}{\delta}} = z^{p-1} = \mathfrak{G}p + r^{\frac{p-1}{\delta}}$$

und, da nach dem Fermatschen Lehrsatz (§. 40.) $z^{p-1} = \mathfrak{S}p+1$ ist, für *jedes* z:

$$19. \quad \mathfrak{S}p + r^{\frac{p-1}{\delta}} = \mathfrak{S}p+1;$$

woraus (17.) folgt.

C. Nun ist es eine Bedingung für die $\frac{p-1}{\delta}$ten *Stammwurzeln* z, dafs

$$20. \quad z^{\frac{p-1}{\delta}} = \mathfrak{S}p+1$$

sei: also *kann jedes* r in (17.) eine $\frac{p-1}{\delta}$te Stammwurzel sein. Und zwar eignen sich *keine andern* Zahlen z als die r zu $\frac{p-1}{\delta}$ten Stammwurzeln; denn *jede* Stammwurzel z mufs $z^{\frac{p-1}{\delta}} = \mathfrak{S}p+1$ geben, und giebt sie den Rest 1, so ist sie auch nach (17.) ein r; denn *alle* r geben diesen Rest.

D. Aber *nicht alle* die r in (17.) sind $\frac{p-1}{\delta}$te Stammwurzeln aus 1 zu p, weil schon *niedrigere* Potenzen als die $\frac{p-1}{\delta}$ten von r den Rest 1 zu p lassen können; und zwar sind alle diejenigen, und *nur* diejenigen r, welche mit Exponenten, die in $\frac{p-1}{\delta}$ *aufgehen*, schon den Rest 1 zu p lassen, *nicht* $\frac{p-1}{\delta}$te Stammwurzeln. Denn gesetzt es sei

$$21. \quad \frac{p-1}{\delta} = \varkappa\sigma,$$

so dafs $\varkappa$ in $\frac{p-1}{\delta}$ aufgeht, so ist, wenn schon

$$22. \quad r^{\varkappa} = \mathfrak{S}p+1$$

giebt, r *nicht* eine $\frac{p-1}{\delta}$te, sondern *kann* schon eine $\varkappa$te Stammwurzel sein, oder selbst eine Stammwurzel für einen *noch niedrigern,* in $\varkappa$ aufgehenden Exponenten. Hingegen kann, wenn z eine $\varkappa$te Stammwurzel, also

$$23. \quad z^{\varkappa} = \mathfrak{S}p+1$$

ist und $\varkappa$ *nicht* in $\frac{p-1}{\delta}$ aufgeht, also etwa

$$24. \quad \frac{p-1}{\delta} = \varkappa\sigma + \varrho$$

ist, wo $\varrho < \varkappa$, dieses z keines der r in (17.) sein. Denn da z eine $\varkappa$te Stammwurzel sein soll, so geben alle die Potenzen z^1, z^2, z^3, ... $z^{\varkappa-1}$, also auch z^{ϱ}, *nicht den Rest* 1. Aus (23.) und (24.) aber ist

$$25. \quad z^{\frac{p-1}{\delta}} = z^{\varkappa\sigma+\varrho} = z^{\varkappa\sigma} z^{\varrho} = (\mathfrak{S}p+1)^{\sigma} z^{\varrho} = \mathfrak{S}p + z^{\varrho},$$

und z^ϱ ist *nicht* $= \mathfrak{S}p+1$: also ist auch $z^{\frac{p-1}{\delta}}$ in (25.) *nicht* $= \mathfrak{S}p+1$; wie es für *alle* r in (17.) sein mufs; so dafs also z *keins* der r in (17.) sein kann.

Also alle r, welche schon mit Exponenten, die in $\frac{p-1}{\delta}$ *aufgehen*, und nur mit *solchen* Exponenten, den Rest 1 zu p lassen, sind *nicht* $\frac{p-1}{\delta}$te Stammwurzeln, und man mufs sie folglich von den r, die der Gleichung (17.) genugthun, *ausschliefsen.*

E. Es ist aber nur nöthig, diejenigen r auszuschliefsen, welche mit dem *höchsten* in $\frac{p-1}{\delta}$ *aufgehenden* Fxponenten schon den Rest 1 zu p lassen; denn wenn ein *niedrigerer* in $\frac{p-1}{\delta}$ aufgehender Exponent $\varkappa$ schon

$$26. \quad r^{\varkappa} = \mathfrak{S}p+1$$

giebt, so ist auch für *das selbe r:*

$$27. \quad r^{2\varkappa},\ r^{3\varkappa},\ \ldots \text{ bis zu } r^{\frac{p-1}{\delta}} = \mathfrak{S}p+1.$$

F. Die *höchsten* in $\frac{p-1}{\delta}$ aufgehenden Exponenten sind aber offenbar $\frac{p-1}{\delta\lambda_1}$, $\frac{p-1}{\delta\lambda_2}$, $\frac{p-1}{\delta\lambda_3}$ etc.; denn die Quotienten von $\frac{p-1}{\delta}$ durch selbige sind

$$28. \quad \frac{p-1}{\delta} : \frac{p-1}{\delta\lambda_1} = \lambda_1, \quad \frac{p-1}{\delta} : \frac{p-1}{\delta\lambda_2} = \lambda_2, \quad \frac{p-1}{\delta} : \frac{p-1}{\delta\lambda_3} = \lambda_3, \ \ldots,$$

und diese Quotienten $\lambda_1, \lambda_2, \lambda_3, \ldots$ sind *Stammzahlen,* und folglich nicht weiter theilbar.

G. Diejenigen r nun, welche

$$29. \quad r^{\frac{p-1}{\delta\lambda_1}} = \mathfrak{S}p+1, \quad r^{\frac{p-1}{\delta\lambda_2}} = \mathfrak{S}p+1, \quad r^{\frac{p-1}{\delta\lambda_3}} = \mathfrak{S}p+1, \quad \ldots$$

geben, sind die ϱ in (4.), die zufolge (I.), wenn man nemlich in (2.) λ_1, $\lambda_2, \lambda_3, \ldots$ statt μ setzt, unter den Werthen von r in (1.) mitbegriffen sind. Denn es giebt (4.), wenn man darin die $\frac{p-1}{\delta\lambda_1}, \frac{p-1}{\delta\lambda_2}, \frac{p-1}{\delta\lambda_3}, \ldots$ten Potenzen nimmt:

$$30. \quad \begin{cases} z^{\frac{p-1}{\delta\lambda_1}\cdot\delta\lambda_1} = z^{p-1} = \mathfrak{S}p + r^{\frac{p-1}{\delta\lambda_1}}, \\ z^{\frac{p-1}{\delta\lambda_2}\cdot\delta\lambda_2} = z^{p-1} = \mathfrak{S}p + r^{\frac{p-1}{\delta\lambda_2}}, \\ z^{\frac{p-1}{\delta\lambda_3}\cdot\delta\lambda_3} = z^{p-1} = \mathfrak{S}p + r^{\frac{p-1}{\delta\lambda_3}}, \\ \ldots\ldots\ldots\ldots\ldots, \end{cases}$$

woraus, da nach dem Fermatschen Lehrsatz (§. 40.) $z^{p-1} = \mathfrak{S}p + 1$ ist,

$$31. \quad \varrho^{\frac{p-1}{\delta\lambda_1}} = \mathfrak{S}p+1, \quad \varrho^{\frac{p-1}{\delta\lambda_2}} = \mathfrak{S}p+1, \quad \varrho^{\frac{p-1}{\delta\lambda_3}} = \mathfrak{S}p+1, \quad \ldots.$$

folgt.

Man darf also nur die Werthe der ϱ in (4.) von den Werthen der r in (1.) *ausschliefsen*, so erhält man die $\frac{p-1}{\delta}$ten *Stammwurzeln* aus 1 zu p. Dieses ist was (II.) behauptet.

Beweis von III. *H.* Was (III.) aussagt, folgt unmittelbar aus (II.) für den besondern Fall $\delta = 1$: denn in diesem Fall sind die r in (1.) alle die Zahlen 1, 2, 3, 4, ... $p-1$ selbst.

Beweis von IV. *I.* Wie in (*D.*) bewiesen, sind diejenigen r in (1.), von welchen schon Potenzen mit Exponenten x, die in $\frac{p-1}{\delta}$ *aufgehen*, und *nur* mit *solchen* Exponenten,

$$32. \quad r^x = \mathfrak{S}p+1$$

geben, *nicht* $\frac{p-1}{\delta}$te Stammwurzeln. Nimmt man also von allen den Werthen von r in (1.) alle diejenigen Potenzen, deren Exponenten x in $\frac{p-1}{\delta}$ *aufgehen*, so sind die r, welche in (5.) $R=1$ geben, von den r in (1.) *auszuschliefsen;* die übrig bleibenden r sind $\frac{p-1}{\delta}$te *Stammwurzeln*; gemäfs (IV.).

Anm. *K.* Die gegenwärtigen Sätze beruhen auf (§. 40. 54. und 55.), und nächstdem auf den besondern Erwägungen in dem Beweise.

§. 65.

Lehrsatz.

I. *Diejenigen von den Zahlen* 1, 2, 3, 4, ... z (z = 2 *ausgenommen*), *welche mit* z *keinen Theiler* > 1 *gemein haben, sind immer paarweise vorhanden, und die Summe jedes solchen Paares ist* = z.

II. *Die Summe aller zu* z *theilerfremden Zahlen* (z = 2 *ausgenommen*) *geht mit* z *auf.*

III. *Das Product jeder zwei zu einander theilerfremden Theiler einer beliebigen Zahl* z *kann kleiner, aber nicht gröfser sein als* z.

Beispiel. Es sei $z = 180$. Die zu dieser Zahl theilerfremden Zahlen sind

1.	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59	61	67	71	73	77	79	83	89
	179	173	169	167	163	161	157	151	149	143	139	137	133	131	127	121	119	113	109	107	103	101	97	91.

Die Zahlen stehen paarweise unter einander; und von jedem Paar ist die Summe $= z$; gemäfs (I.).

Die Summe aller der Zahlen (1.) ist 4320; was mit $z = 180$ aufgeht; gemäfs II.

Die verschiedenen *Theiler* von z sind folgende:

2. 1 2 3 4 5 6 9 10 12 15 18 20 30 36 45 60 90.

Die Producte der zu einander *theilerfremden* Theiler sind

$$3.\quad \begin{cases} 2.\,3 = 6, & 2.\,5 = 10, & 2.\,9 = 18, & 2.15 = 30, & 2.45 = 90; \\ 3.\,4 = 12, & 3.\,5 = 15, & 3.10 = 30, & 3.20 = 60; \\ 4.\,5 = 20, & 4.\,9 = 36, & 4.15 = 60, & 4.45 = 180; \\ 5.\,6 = 30, & 5.12 = 60, & 5.36 = 180; \\ 9.10 = 90, & 9.20 = 180. \end{cases}$$

Keins dieser Producte ist gröfser als $z = 180$; gemäfs (III.).

Beweis. *A.* Wenn die Zahl $a > 0 < z$ zu z theilerfremd ist, so ist es nothwendig auch $z - a = b$: denn ginge eine Zahl > 1 in b und z zugleich auf, so ginge sie auch nothwendig in a auf (§. 18.). Also ist zu jeder zu z theilerfremden Zahl a eine andere $b > 0 < z$ vorhanden, die ebenfalls mit z keinen Theiler > 1 gemein hat. Die zu z theilerfremden Zahlen > 0 und $< z$ sind also immer *paarweise* vorhanden, und die Summe jedes solchen Paares a und b ist $a + b = z$; gemäfs (I.).

B. Da die Summe jedes *Paares* der zu z theilerfremden Zahlen z ausmacht, so ist die Summe *aller* ein *Vielfaches* von z, und geht also mit z auf; gemäfs (II.).

C. *a.* Es seien δ_1 und δ_2 zwei zu einander *theilerfremde* Theiler von z, und es sei, wenn es möglich ist, ihr Product $\delta_1\delta_2 > z$, also etwa

$$4.\quad \delta_1\delta_2 = nz + r;$$

wo durch n immer $r < z$ gemacht werden kann, weswegen denn $r < \delta_1\delta_2$ vorausgesetzt werden darf.

b. Da nun z sowohl mit δ_1, als mit δ_2 aufgehen soll, so mufs nach (§. 18.) in (4.) auch nothwendig r sowohl mit δ_1, als mit δ_2, also nach (§. 26.) mit $\delta_1\delta_2$ aufgehen. Aber r ist nothwendig $< \delta_1\delta_2$ (*a.*), also kann r nur 0 sein und folglich nur

$$5.\quad \delta_1\delta_2 = nz$$

gesetzt werden.

c. Kann nun $n > 1$ sein, so mufs vermöge (5.) n entweder in δ_1 oder in δ_2 aufgehen; oder auch irgend ein *Theiler* n_1 von n mufs in δ_1, der

andere Theiler n_2, welcher $n_1 n_2 = n$ giebt, mufs in δ_2 aufgehen. Ist $n_1 = n_2$, so mufs n selbst in δ_1 oder δ_2 aufgehen, denn δ_1 und δ_2 haben nach der Voraussetzung keinen Theiler $n_1 = n_2 > 1$ gemein.

d. Also zunächst für *gleiche* Theiler von n mufs die Gleichung (5.) so wie sie ist stattfinden. Geht dann n etwa in δ_1 auf, so folgt daraus

$$6. \quad \frac{\delta_1}{n} . \delta_2 = z.$$

Dieses durch δ_1 dividirt giebt

$$7. \quad \frac{\delta_2}{n} = \frac{z}{\delta_1},$$

hier ist $\frac{z}{\delta_1}$ eine *ganze* Zahl, $\frac{\delta_2}{n}$ aber *nicht*, weil δ_1 und δ_2 den Theiler $n > 1$ *nicht* gemein haben. Also kann für *gleiche* Theiler von n, (7.) nur für $n = 1$ stattfinden, und also n nicht > 1, mithin in (5.) $\delta_1 \delta_2$ nicht $> z$ sein.

e. Für *ungleiche* Theiler n_1 und n_2 von n würde (5.)

$$8. \quad \delta_1 \delta_2 = n_1 n_2 z$$

geben, und, wenn nun n_1 in δ_1, n_2 in δ_2 aufgehend angenommen wird,

$$9. \quad \frac{\delta_1}{n_1} . \frac{\delta_2}{n_2} = z.$$

Dies durch δ_1 oder δ_2 dividirt giebt

$$10. \quad \frac{\delta_2}{n_1 n_2} = \frac{z}{\delta_1} \text{ und } \frac{\delta_1}{n_1 n_2} = \frac{z}{\delta_2},$$

hier sind $\frac{z}{\delta_1}$ und $\frac{z}{\delta_2}$ *ganze* Zahlen, $\frac{\delta_2}{n_1 n_2}$ und $\frac{\delta_1}{n_1 n_2}$ aber sind es *nicht*, weil δ_2 zwar mit n_2, aber nicht mit dem Theiler n_1 von δ_1, und δ_1 zwar mit n_1, aber nicht mit dem Theiler n_2 von δ_2 aufgeht. Die erste Gleichung (10) findet also nur Statt für $n_1 = 1$ und die zweite nur für $n_2 = 1$, mithin (8.) nur für $n_1 n_2$ oder $n = 1$. Also auch in diesem Fall kann in (5.) n nicht gröfser sein als 1, und folglich $\delta_1 \delta_2$ nicht gröfser als z. Also kann überhaupt $\delta_1 \delta_2$ nicht gröfser als z sein; gemäfs (III.).

§. 66.

Lehrsatz.

Wenn* p *eine ungerade Stammzahl ist, so ist

I. ***Für jede Stammwurzel*** z_δ ***aus*** 1 ***zu*** p ***mit geradem Exponenten*** δ, ***also, da*** p—1 ***immer gerade ist, auch für jede*** p—1***te oder Hauptstammwurzel:***

$$1. \quad z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}\,p - 1.$$

Aber nur allein für den Exponenten $\frac{1}{2}\delta$, *und für keinen andern Exponenten* $<\delta$, *ist zu* p *der Rest* $=-1$.

II. *Von allen Stammwurzeln* z_δ *aus* 1 *zu* p *mit ungeradem Exponenten* δ *giebt keine der Potenzen* $z_\delta^1, z_\delta^2, z_\delta^3, \ldots$ *bis* z_δ^δ *zu* p *den Rest* -1.

III. *a. Alle Hauptstammwurzeln aus* 1 *zu* p *sind Nichtquadratreste zu* p.

b. Alle $\frac{p-1}{\lambda}=\delta$*ten Stammwurzeln aus* 1 *zu* p *sind, wenn* λ *eine Stammzahl ist,* λ*te Reste zu* p, *das heifst Werthe von* r *in*

$$2. \quad z^\lambda = \mathfrak{G}p + r.$$

c. Alle $\frac{p-1}{\varkappa}=\delta$*ten Stammwurzeln aus* 1 *zu* p *sind, wenn* $\varkappa$ *nicht eine Stammzahl ist,* λ*te Reste* r *zu* p *in* (2.), *wenn* λ *eine der Stammzahlen ist, die in* $\varkappa$ *aufgehen.*

d. Nur dann sind alle Nichtquadratreste zu p, $p-1$ *ausgenommen, Hauptstammwurzeln aus* 1 *zu* p, *wenn* $p-1$ *mit keiner andern Stammzahl als* 2 *und mit* $\frac{1}{2}(p-1)$ *aufgeht. Sonst nicht.*

e. Für kein $\varkappa$ *sind in*

$$3. \quad z^\varkappa = \mathfrak{G}p + r$$

alle r *für* $z=1,2,3,4,\ldots p-1$, $\frac{p-1}{\varkappa}=\delta$*te Stammwurzeln.*

IV. *Für jede Stammzahl* p *und für jedes* δ *sind die* δ*ten Stammwurzeln aus* 1 *zu* p *für ein und dasselbe* δ *entweder sämmtlich Quadratreste, oder sämmtlich Nichtquadratreste; nicht zum Theil Quadratreste, zum Theil Nichtquadratreste. Desgleichen ist das Product jeder geraden Zahl von* δ*ten Stammwurzeln aus* 1 *zu* p *für jedes* p *und* δ *ein Quadratrest zu* p.

V. *Wenn man für eine Stammwurzel* z_δ *aus* 1 *zu* p *mit geradem Exponenten* δ, *also auch für eine Hauptstammwurzel,*

$$4. \quad z_\delta^\varkappa = \mathfrak{G}p + r$$

setzt, wo $\varkappa < \frac{1}{2}\delta$, *so ist*

$$5. \quad z_\delta^{\frac{1}{2}\delta+\varkappa} = \mathfrak{G}p - r;$$

so dafs man also die Reste zu allen Potenzen $z_\delta^{\frac{1}{2}\delta+\varkappa}$ *findet, wenn man diejenigen zu* $z^\varkappa$ *von* p *abzieht.*

VI. *Ist der Exponent* δ *einer Stammwurzel* z_δ *aus* 1 *zu* p *eine ungerade Zahl, so ist* $p-z_\delta$ *eine* 2δ*te Stammwurzel aus* 1 *zu* p.

VII. *Wenn in*

$$6.\quad z^{\varkappa} = \mathfrak{G}p + r$$

$\varkappa$ die ***Theiler*** *von δ bezeichnet, so dafs also $\varkappa$ auch δ selbst sein kann: wenn ferner δ* ***gerade*** *ist, und der Rest* r *für $\varkappa = \frac{1}{2}\delta$ ist gleich -1, für alle andern $\varkappa$ dagegen, die* ***nur*** *in δ* ***und nicht*** *in $\frac{1}{2}\delta$ aufgehen, weder $+1$, noch -1, so ist* z *nothwendig eine δte* ***Stammwurzel*** *aus* 1 *zu* p.

Findet nicht ***beides zugleich*** *Statt, so ist* z ***nicht*** *eine δte Stammwurzel aus* 1 *zu* p.

VIII. *a. Wenn der Exponent δ einer δten Stammwurzel z_δ aus* 1 *zu* p *mit* 4 *aufgeht, so ist auch* $p - z$ *eine δte* ***Stammwurzel*** *aus* 1 *zu* p.

b. Geht δ nur mit 2, *nicht mit* 4 *auf, so ist* $p - z$ *eine $\frac{1}{2}\delta$te* ***Stammwurzel*** *aus* 1 *zu* p; *so dafs es also für alle mit* 2 *und nicht mit* 4 *aufgehenden δ* ***eben so viele*** *$\frac{1}{2}\delta$te als δte Stammwurzeln aus* 1 *zu* p *giebt.*

IX. *Wenn z_δ eine δte und z_ε eine εte* ***Stammwurzel*** *aus* 1 *zu* p *ist, und δ und ε sind zu einander* ***theilerfremd,*** *so ist in*

$$7.\quad z_\delta . z_\varepsilon = \mathfrak{G}p + r,$$

wenn $r > 1$ ist, r *eine $\delta\varepsilon$te* ***Stammwurzel*** *aus* 1 *zu* p, *und $\delta\varepsilon$ ist nie gröfser als* $p-1$ (§. 65. III.).

X. *Wenn in*

$$8.\quad z_\delta^{\varkappa} = \mathfrak{G}p + r,$$

$$9.\quad x^{\lambda} = \mathfrak{G}p + z_\delta,$$

z *eine δte* ***Stammwurzel*** *aus* 1 *zu* p *ist, und unter den Resten* r *in* (8.), *für die verschiedenen $\varkappa = 1, 2, 3, \ldots\ \delta - 1$, kommt weder* $x - \mathfrak{G}p$, *noch* $x^2 - \mathfrak{G}p$, *noch* $x^3 - \mathfrak{G}p, \ldots,$ *bis zu* $x^{\lambda-1} - \mathfrak{G}p$ *vor, so ist* x *eine $\lambda\varkappa$te* ***Stammwurzel*** *aus* 1 *zu* p.

Beispiele. Aus Taf. I. Zu I. Für die $\delta = 4$te Stammwurzel 11 ist $11^{\frac{1}{2}\delta} = 11^2 = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$. Für die $\delta = 6$te Stammwurzel 14 ist $14^{\frac{1}{2}\delta} = 14^3 = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$. Für die $\delta = 20$te Stammwurzel 37 ist $37^{\frac{1}{2}\delta} = 37^{10} = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$, u. s. w. Kein anderer aber als der Exponent $\frac{1}{2}\delta$ giebt zu p den Rest 60 oder -1.

Zu II. Zu der $\delta = 3$ten Stammwurzel 13 sind die Reste 13 und 47; zu der $\delta = 5$ten Stammwurzel 34 sind die Reste 34, 58, 20 und 9; für die $\delta = 15$te Stammwurzel 16 sind die Reste 16, 12, 9, 22, 47, 20, 15, 57, 58, 13, 25, 34, 56 und 42, u. s. w. Keiner dieser Reste ist 60 oder -1; gemäfs (II.).

Zu III. Die Zahlen in der *zweiten* horizontalen Zeile der Tafel sind die *Quadratreste* zu *p*. Unter ihnen findet sich *keine* der Hauptstammwurzeln 2, 6, 7, 10, 17 etc.; also sind alle Hauptstammwurzeln *Nichtquadratreste* zu *p*; gemäfs (III. *a*.).

Dagegen finden sich alle die $\frac{p-1}{2} = 30$ten Stammwurzeln 4, 5, 19, 36 etc. unter den Zahlen der *zweiten* horizontalen Zeile der Tafel, und sind also alle *zweite* oder *Quadratreste* zu *p*. Die Zahlen der *dritten* horizontalen Zeile sind die $\lambda = 3$*ten Reste* zu *p*. Unter ihnen befinden sich in $\frac{p-1}{3} = 20$ten Stammwurzeln 8, 23, 24 etc. Die Zahlen der *fünften* horizontalen Zeile sind die $\lambda = 5$*ten Reste* zu *p*. Unter ihnen befinden sich die $\frac{p-1}{5} = 12$ten Stammwurzeln 21, 29, 32 etc. Ferner befinden sich z. B. die $\frac{p-1}{\varkappa} = \frac{p-1}{6} = 10$ten Stammwurzeln 3, 27, 41 unter den Zahlen der 3ten horizontalen Zeile; u. s. w.; gemäfs (III. *b*. und *c*.). Aber *nicht alle* Zahlen, die in der zweiten horizontalen Zeile *nicht* stehen, also nicht alle Nichtquadratreste, sind Hauptstammwurzeln; und *nicht alle* Zahlen der 3ten, 5ten Zeile etc. sind $\frac{p-1}{3}$, $\frac{p-1}{5}$, $\frac{p-1}{6}$te etc. Stammwurzeln.

Zu III. *d*. giebt die am Ende dieses Bandes angehängte Tafel Beispiele. Für $p = 23$ geht $p-1$ nur mit den Stammzahlen 2 und $11 = \frac{1}{2}(p-1)$ auf. Die *Nichtquadratreste* zu $p = 23$ sind 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 und 22. Alle diese Zahlen, $p-1 = 22$ ausgenommen, sind Hauptstammwurzeln aus 1 zu $p = 23$.

Hier in Tafel I. sind z. B. für $\varkappa = 6$ die verschiedenen Werthe von *r* in (3.) folgende: 1, 3, 9, 20, 27, 34, 41, 52, 58 und 60. Nicht diese Zahlen *alle*, sondern nur die vier: 3, 27, 41 und 52 sind $\frac{p-1}{\varkappa} = \frac{60}{6} = 10$te Stammwurzeln aus 1 zu *p*; gemäfs (III. *e*.).

Zu IV. Nach Tafel I. sind z. B. die 20ten Stammwurzeln 8, 23, 24, 28, 33, 37, 38 und 53 *sämmtlich Nichtquadratreste*; denn sie finden sich nicht unter den Zahlen der zweiten horizontalen Zeile der Tafel. Dagegen die 15ten Stammwurzeln 12, 15, 16, 22, 25, 42, 56 und 57 sind *sämmtlich Quadratreste*; gemäfs (IV.).

Zu V. Für die $\delta = 10$te Stammwurzel $z = 27$ aus 1 zu $p = 61$ ist z. B. $z^{\varkappa} = z^3 = \mathfrak{G}p + 41$, also in (4.) $r = 41$, und $z^{\frac{1}{2}\delta+\varkappa} = z^8$ ist $= \mathfrak{G}p + 20 = \mathfrak{G}p - 41 = \mathfrak{G}p - r$. Für die $\delta = 30$te Stammwurzel $z = 39$ ist z. B.

$z^{\varkappa} = z^{11} = \mathfrak{G}p + 19$, also $r = 19$; $z^{\frac{1}{2}\delta+\varkappa} = z^{26}$ ist $= \mathfrak{G}p + 42 = \mathfrak{G}p - 19 = \mathfrak{G}p - r$. Für die Hauptstammwurzel $z = 43$ ist z. B. $z^{\varkappa} = z^{14} = \mathfrak{G}p + 4$, also $r = 4$; und $z^{\frac{1}{2}\delta+\varkappa} = z^{44}$ ist $= \mathfrak{G}p + 57 = \mathfrak{G}p - 4 = \mathfrak{G}p - r$ etc.; gemäfs (V.).

Zu VI. $z = 13$ ist eine Stammwurzel aus 1 zu p mit der ***ungeraden*** Zahl 3 zum Exponenten; und $p - z = 48$ ist eine $2\delta = 6$te Stammwurzel aus 1 zu p. $z = 20$ ist eine Stammwurzel mit der ***ungeraden*** Zahl 5 zum Exponenten; und $p - z = 41$ ist eine $2\delta = 10$te Stammwurzel aus 1 zu p; gemäfs (VI.).

Zu VII. Von $\delta = 20$ sind die Theiler $\varkappa = 1, 2, 4, 5$ und 10. Davon ist derjenige, welcher ***nur*** in δ, ***nicht*** in $\frac{1}{2}\delta = 10$ aufgeht, 4. Für $z = 28$ ist $z^{\frac{1}{2}\delta} = z^{10} = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$ und $z^4 = \mathfrak{G}p + 20$. Also ist r in (6.) $= -1$ für $\varkappa = \frac{1}{2}\delta$ und weder $+1$ noch -1 für das $\varkappa$, welches nicht in $\frac{1}{2}\delta$ aufgeht; und $z = 28$ ist eine 20te Stammwurzel aus 1 zu p.

Dagegen ist für $z = 11$ zwar $z^{10} = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$, aber z^4 ist $= \mathfrak{G}p + 1$, und $z = 11$ ist ***nicht*** eine 20te Stammwurzel; gemäfs (VII.).

Zu VIII. Für $\delta = 20$ sind $z_\delta = 8, 23, 24, 28$ Stammwurzeln aus 1 zu p. δ geht ***mit*** 4 ***auf***, und $p - (8, 23, 24, 28) = 53, 38, 37$ und 33 sind ebenfalls 20te Stammwurzeln aus 1 zu p; gemäfs (VIII. *a.*).

Die $\delta = 30$ten Stammwurzeln aus 1 zu p sind $z = 4, 5, 19, 36, 39, 45, 46$ und 49. Hier geht δ ***nur mit*** 2, ***nicht*** mit 4 auf, und $p - (4, 5, 19, 36, 39, 45, 46, 49) = 57, 56, 42, 25, 22, 16, 15$ und 12 sind die $\frac{1}{2}\delta = 15$ten Stammwurzeln aus 1 zu p; gemäfs (VIII. *b.*).

Zu IX. $z_\delta = 11$ ist eine $\delta = 4$te und $z_\varepsilon = 42$ eine $\varepsilon = 15$te Stammwurzel aus 1 zu p. δ und ε sind zu einander theilerfremd, und (7.) giebt hier $z_\delta z_\varepsilon = 11 . 42 = 462 = \mathfrak{G}p + 35$, also $r = 35$; und dieses $r = 35$ ist eine $4 . 15 = 60$te oder Hauptstammwurzel; gemäfs (IX.).

Zu X. $z_\delta = 22$ ist eine $\delta = 15$te Stammwurzel aus 1 zu p, und $12^2 = \mathfrak{G}p + 22$, also in (9.) $x = 12$. Die Reste r in (8.) zu $z = 22$ sind für $\varkappa = 1, 2, 3, \ldots 14$, $r = 22, 57, 34, 16, 47, 58, 56, 12, \ldots$ etc. Unter denselben ***kommt*** $x = 12$ ***vor***, also ist $x = 12$ ***nicht*** eine $\lambda\delta = 4 . 15 = 60$te Stammwurzel aus 1 zu p. In der That ist 12 nur eine 12te Stammwurzel aus 1 zu p. Dagegen ist $z_\delta = 29$ eine $\delta = 12$te Stammwurzel aus 1 zu p, und $6^5 = \mathfrak{G}p + 29$, also in (9.) $x = 6$. Die Reste r in (8.) zu $z = 29$ sind 29, 48, 50, 47, 21, 60, 32, 13, 11, 14, 40. Unter denselben kommt weder $x = 6$,

28 *

noch $x^2 = \mathfrak{G}p+36$, noch $x^3 = \mathfrak{G}p+33$, noch $x^4 = \mathfrak{G}p+15$ vor; also mufs $x=6$ eine $5.12=60$te Stammwurzel aus 1 zu p sein; was auch der Fall ist; gemäfs (X.).

Beweis von I. *A.* Für eine δte Stammwurzel aus 1 zu p ist $z^\delta = \mathfrak{G}p+1$ oder

$$10. \quad z_\delta^\delta - 1 = \mathfrak{G}p.$$

Dieses giebt, wenn δ *gerade*, also $\frac{1}{2}\delta$ eine *ganze* Zahl ist,

$$11. \quad (z_\delta^{\frac{1}{2}\delta}-1)(z_\delta^{\frac{1}{2}\delta}+1) = \mathfrak{G}p:$$

also mufs p entweder in $z_\delta^{\frac{1}{2}\delta}-1$, oder in $z_\delta^{\frac{1}{2}\delta}+1$ *aufgehen*, das heifst, es mufs

$$12. \quad \text{entweder } z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p+1,$$

$$13. \quad \text{oder } z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p-1$$

sein. Das Erste (12.) kann nicht sein, denn sonst gäbe nicht erst die δte, sondern schon die $\frac{1}{2}\delta$te Potenz von z_δ zu p den Rest $+1$, und z_δ wäre also keine δte *Stammwurzel*. Mithin mufs die Gleichung (13.) stattfinden; und diese ist die (1.) des Lehrsatzes.

B. Wäre noch für einen andern Exponenten als $\frac{1}{2}\delta$, z. B. für den Exponenten $\varepsilon<\delta$,

$$14. \quad z_\delta^\varepsilon = \mathfrak{G}p-1,$$

so wäre

$$15. \quad z_\delta^{2\varepsilon} = \mathfrak{G}p+1.$$

Aber 2ε ist *nicht* $=\delta$, sondern entweder kleiner oder gröfser als δ, jedoch $<2\delta$. Setzt man für den zweiten Fall $2\varepsilon=\delta+\varkappa$, wo nun $\varkappa<\delta$ ist, so wäre

$$16. \quad z_\delta^{2\varepsilon} = z_\delta^{\delta+\varkappa} = z_\delta^\delta z_\delta^\varkappa = (\mathfrak{G}p+1)z_\delta^\varkappa = \mathfrak{G}p+z_\delta^\varkappa,$$

also müfste, wenn nach (15.) $z_\delta^{2\varepsilon}=\mathfrak{G}p+1$ sein sollte, $\mathfrak{G}p+z_\delta^\varkappa=\mathfrak{G}p+1$ oder

$$17. \quad z_\delta^\varkappa = \mathfrak{G}p+1$$

sein. Aber für *keinen* Exponenten, der kleiner ist als δ, ist der Rest der Potenz zu p gleich $+1$, weil z_δ eine δte *Stammwurzel* sein soll. Also kann die Gleichung (15.) weder für $2\varepsilon<\delta$, noch, in der Form (17.), für $2\varepsilon>\delta$ $<2\delta$ stattfinden, und folglich auch nicht die Gleichung (14.), und es giebt mithin *kein* anderer Exponent ε, als $\frac{1}{2}\delta$, für die δte Stammwurzel z_δ, $z_\delta^\varepsilon=\mathfrak{G}p-1$; gemäfs (I.).

Bew. von II. *C.* Ist δ *ungerade,* und wäre für einen andern Exponenten als δ, z. B. für $\varepsilon<\delta$, $z_\delta^\varepsilon=\mathfrak{G}p-1$, so müfste wieder, wie in (15.), $z_\delta^{2\varepsilon}=\mathfrak{G}p+1$ sein; und da 2ε *nicht* $=\delta$ sein kann, sondern entweder $<\delta$

oder $>\delta<2\delta$ ist, so folgt, ganz wie in (*B.*), dafs für *kein* $\varepsilon<\delta$ die δte Stammwurzel z_δ, $z_\delta^\varepsilon=\mathfrak{G}p-1$ geben kann; gemäfs (II.).

Bew. von III. *a.* *D.* Die *Hauptstammwurzeln* z_{p-1}, für welche

$$18.\quad z_{p-1}^{p-1}=\mathfrak{G}p+1$$

sein mufs, können nicht unter den *Quadratresten* r zu p sein, für welche $z^2=\mathfrak{G}p+r$ ist: denn nach (§. 49. 1.) ist für die *Quadratreste* r schon

$$19.\quad r^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1,$$

also *schon* ihre $\frac{1}{2}(p-1)$te Potenz läfst zu p den Rest 1; was für $p-1$te Stammwurzeln nicht der Fall ist. Da es aber nun *jedenfalls* Hauptstammwurzeln *giebt,* so können sich dieselben nur unter den *Nichtquadratresten* ϱ befinden; gemäfs (III. *a.*).

Bew. von III. *b.* *E.* Die Gleichung (2.) giebt, wenn man die $\frac{p-1}{\lambda}$te Potenz nimmt,

$$20.\quad z^{\frac{p-1}{\lambda}.\lambda}=z^{p-1}=\mathfrak{G}p+r^{\frac{p-1}{\lambda}}$$

und, da für *jedes* z nach dem Fermatschen Lehrsatz (§. 40.) $z^{p-1}=\mathfrak{G}p+1$ ist,

$$21.\quad r^{\frac{p-1}{\lambda}}=\mathfrak{G}p+1.$$

Dieses ist eine der Bedingungen für die $\frac{p-1}{\lambda}=\delta$ten Stammwurzeln z_δ: also müssen sich alle $\frac{p-1}{\lambda}=\delta$ten Stammwurzeln z_δ unter den λten Resten r in (2.) finden; gemäfs (III. *b.*).

Bew. von III. *c.* *F.* Wenn z eine $\delta=\frac{p-1}{\varkappa}$te Stammwurzel aus 1 zu p sein soll, so mufs

$$22.\quad z^{\frac{p-1}{\varkappa}}=\mathfrak{G}p+1$$

sein; also: wenn λ eine der in $\varkappa$ *aufgehenden* Stammzahlen ist, und man setzt etwa

$$23.\quad \varkappa=\mu\lambda,$$

so mufs

$$24.\quad z^{\frac{p-1}{\mu\lambda}}=\mathfrak{G}p+1,$$

also auch

$$25.\quad z^{\frac{p-1}{\lambda}}=(\mathfrak{G}p+1)^\mu=\mathfrak{G}p+1$$

sein. Diese Bedingung erfüllen die r in (2.) gemäfs (21.). Also *müssen* sich alle $\delta=\frac{p-1}{\varkappa}$ten Stammwurzeln unter den λten Resten r in (2.) finden.

Bew. von III. *d.* *G.* *α.* Es giebt immer $\frac{1}{2}(p-1)$ ***Nichtquadratreste*** (§. 45. III.), und nach (§. 63. I.) giebt es so viele ***Hauptstammwurzeln*** als Zahlen >0 und $<p$ zu $p-1$ theilerfremd sind.

β. Nun ist $p-1$ ***immer gerade***, also sind die $\frac{1}{2}(p-1)$ Zahlen 2, 2.2, 3.2, 4.2, ... $\frac{1}{2}(p-1).2=p-1$ zu $p-1$ ***nicht*** theilerfremd, sondern haben damit den Theiler $2>1$ gemein. Es bleiben von den gesammten $p-1$ Zahlen 1, 2, 3, 4, ... $p-1$ nur die $\frac{1}{2}(p-1)$ ***ungeraden*** Zahlen 1, 3, 5, 7, ... $p-1-1$ übrig, die zu $p-1$ theilerfremd sein können. Geht nun $p-1$ nur mit den Stammzahlen 2 und $\frac{1}{2}(p-1)$ auf, so sind sie es mit Ausnahme von $p-1$ ***wirklich;*** denn keine von ihnen geht mit 2 auf. Also giebt es alsdann wirklich $\frac{1}{2}(p-1)-1$ Hauptstammwurzeln, so viele als Nichtquadratreste, mit Ausnahme von $p-1$. Und da nun alle Hauptstammwurzeln Nichtquadratreste sind, so sind alsdann alle Nichtquadratreste, mit Ausnahme von $p-1$, Hauptstammwurzeln.

γ. Geht dagegen $p-1$, aufser mit 2, noch mit andern, also noch mit einer oder mehreren ***ungeraden*** Stammzahlen $q_1, q_2, \ldots < p$ auf, so befinden sich dieselben nothwendig unter den $\frac{1}{2}(p-1)$ ***ungeraden*** Zahlen 1, 3, 5, 7, ... $p-2$, die allein noch zu $p-1$ theilerfremd sein konnten; denn diese ungeraden Zahlen sind diejenigen $<p$ ***alle***, welche es giebt. Es gehen also alsdann schon $q_1, q_2, \ldots$ von jenen $\frac{1}{2}(p-1)$ ungeraden Zahlen ab, und folglich giebt es dann *weniger* oder $\frac{1}{2}(p-1)$ zu $p-1$ theilerfremde Zahlen >0 und $<p$, und mithin auch weniger Hauptstammwurzeln. Mithin sind alsdann ***nicht alle*** Nichtquadratreste Hauptstammwurzeln; gemäfs (III. *d.*).

Bew. von III. ***e.*** Nach (§. 54. I.) hat r in (3.) $\frac{p-1}{\varkappa}=\delta$ ***verschiedene*** Werthe. Andrerseits ist nach (§. 63. I.) die Anzahl der $\frac{p-1}{\varkappa}=\delta$ten Stammwurzeln aus 1 zu p der Anzahl der zu δ ***theilerfremden*** Zahlen gleich. Letztere ist *immer* $<\delta$, selbst wenn δ eine ***Stammzahl*** ist; denn selbst dann sind erst die $\delta-1$ Zahlen 1, 2, 3, 4, ... $\delta-1$ zu δ ***theilerfremd.*** Also sind für ***kein*** $\varkappa$ ***alle*** r in (3.) $\frac{p-1}{\varkappa}=\delta$te Stammwurzeln; gemäfs (III. ***e.***).

Bew. von IV. ***H.*** Alle $\delta=\frac{p-1}{\varkappa}$ten Stammwurzeln z_δ, für ***denselben*** Exponenten δ, finden sich nach (III. ***c.***) unter den Resten r in $z^\lambda = \mathfrak{G}p+r$ für ***denselben*** Exponenten λ, der eine von den in $\varkappa$ aufgehenden ***Stammzahlen*** ist. Diese Reste r sind entweder ***Quadratreste***, oder ***Nichtquadratreste;***

denn andere Zahlen $>0<p$ giebt es nicht. Ist nun eine der δten Stammwurzeln ein r, welches ein *Quadratrest*, also ein Rest *für* $\lambda=2$ *ist*, so sind es auch alle andern δten Stammwurzeln; *denn alle* finden sich unter den r für das *gleiche* λ. Ist eine der δten Stammwurzeln z_1 ein r, welches ein *Nichtquadratrest* ist, so kann keine andere δte Stammwurzel ein *Quadratrest* sein; denn sonst wären es, wie so eben bemerkt, auch *alle andern*, und folglich auch z_1.

Also, wenn eine δte Stammwurzel ein *Quadratrest* ist, so sind es auch alle andern; und wenn eine derselben ein *Nichtquadratrest* ist, sind es ebenfalls alle übrigen.

Das Product jeder *geraden* Anzahl von Quadratresten und Nichtquadratresten ist nach (§. 52. I. und II.) ein *Quadratrest:* also ist das Product jeder *geraden* Anzahl von δten Stammwurzeln für jedes p und δ ein *Quadratrest;* gemäfs (IV.).

Bew. von V. ***F.*** Nach (I.) ist für jedes *gerade* δ

$$26.\quad z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p-1.$$

Setzt man nun, wie in (2.),

$$27.\quad z_\delta^{\varkappa} = \mathfrak{G}p+r,$$

so ergiebt sich, wenn man (26.) mit (27.) multiplicirt,

$$28.\quad z_\delta^{\frac{1}{2}\delta+\varkappa} = \mathfrak{G}p-r = \mathfrak{G}p+(p-r);$$

gemäfs (V.).

Bew. von VI. ***G.*** Es ist

$$29.\quad (p-z)^{2\delta} = \mathfrak{G}p+(-z)^{2\delta} = \mathfrak{G}p+z^{2\delta},$$

indem 2δ *immer* gerade ist. Ist nun z eine δte Stammwurzel aus 1 zu p, so ist

$$30.\quad z_\delta^{\delta} = \mathfrak{G}p+1.$$

Aber es ist

$$31.\quad (p-z_\delta)^{\delta} = \mathfrak{G}p+(-z)^{\delta},$$

also ist, für ein *ungerades* δ,

$$32.\quad (p-z_\delta)^{\delta} = \mathfrak{G}p-z_\delta^{\delta} = \mathfrak{G}p-1 \;\; (30.),$$

und folglich *kann* nach (I.) $p-z_\delta$ eine 2δte Stammwurzel sein; denn ist sie eine solche, so mufs nach (I.) $(p-z_\delta)^{\delta}=\mathfrak{G}p-1$ sein; was nach (32.) der Fall ist.

H. Es ist aber auch, für jeden Exponenten $\varkappa<\delta$,

$$33.\quad (p-z_\delta)^{\varkappa} = \mathfrak{G}p+(-z_\delta)^{\varkappa} = \mathfrak{G}p\pm z_\delta^{\varkappa},$$

je nachdem $\varkappa$ gerade oder ungerade ist. Könnte nun für $\varkappa<\delta$, $(p-z_\delta)^{\varkappa}=\mathfrak{G}p\pm1$ sein, so müfste zufolge (33.)

$$34. \quad z_\delta^\varkappa = \mathfrak{S}p \pm 1$$

sein. Dieses ist nicht der Fall; denn *keine* niedrigere Potenz als δ von der δten Stammwurzel z_δ giebt zu p den Rest $+1$, was auch δ sein mag; und wenn δ *ungerade* ist, giebt auch keine niedrigere Potenz als δ nach (II.) den Rest -1 zu p: also kann r in

$$35. \quad (p - z_\delta)^\varkappa = \mathfrak{S}p + r$$

für kein $\varkappa < \delta$ weder $+1$ noch -1 sein.

I. Multiplicirt man nun (35.) mit (32.), so ergiebt sich

$$36. \quad (p - z_\delta)^{\delta+\varkappa} = \mathfrak{S}p - r:$$

also kann auch keine Potenz von $p - z_\delta$, deren Exponent $> \delta$ und $< 2\delta$ ist, zu p weder $+1$ noch -1 zum Rest geben. Mithin kann überhaupt keine Potenz von $p - z_\delta$, deren Exponent > 0 und $< 2\delta$ ist, zu p den Rest $+1$ lassen; die δte Potenz von $p - z_\delta$ läfst aber nach (32.) zu p den Rest -1: mithin ist $p - z_\delta$ nothwendig eine 2δte Stammwurzel; gemäfs (VI.).

Bew. von VII. *K.* Wenn für einen *geraden* Theiler δ von $p - 1$

$$27. \quad z^{\frac{1}{2}\delta} = \mathfrak{S}p - 1$$

ist, so ist, die zweite Potenz genommen,

$$38. \quad z^\delta = \mathfrak{S}p + 1;$$

also *kann* alsdann dieses z eine δte Stammwurzel z_δ aus 1 zu p sein.

Aber wenn

$$39. \quad \delta = 2\lambda\varkappa$$

und schon

$$40. \quad z^\varkappa = \mathfrak{S}p + 1$$

oder auch

$$41. \quad z^\varkappa = \mathfrak{S}p - 1,$$

also $z^{2\varkappa} = \mathfrak{S}p + 1$ ist, so ist z nicht eine δte, sondern in dem Falle (40.) schon eine $\varkappa$te, und in dem Fall (41.) eine $2\varkappa$te Stammwurzel aus 1 zu p.

Dagegen giebt (40.), vermöge (39.), indem $\frac{1}{2}\delta = \lambda\varkappa$ ist,

$$42. \quad z^{\frac{1}{2}\delta} = z^{\lambda\varkappa} = (\mathfrak{S}p + 1)^\lambda = \mathfrak{S}p + 1;$$

was der vorausgesetzten Gleichung (37.) widerspricht: also kann z für keinen Exponenten $\varkappa$, der in $\frac{1}{2}\delta$ aufgeht, eine $\varkappa$te Stammwurzel sein, sobald nach (37.) $z^{\frac{1}{2}\delta} = \mathfrak{S}p - 1$ ist.

L. Auch für kein anderes $\varkappa$, welches in δ *nicht* aufgeht, kann z eine $\varkappa$te Stammwurzel sein, sobald die Gleichung (37.) stattfindet. Denn gesetzt es sei

$$43. \quad \delta = n\varkappa + e,$$

wo $e > 0$ und $< \varkappa$, so ist, wenn z eine $\varkappa$te Stammwurzel, also

$$44. \quad z^{\varkappa} = \mathfrak{S}p + 1$$

wäre,

$$45. \quad z^{\delta} = z^{n\varkappa+e} = (\mathfrak{S}p+1)^n z^e = \mathfrak{S}p + z^e.$$

Setzt man nun

$$46. \quad z^e = \mathfrak{S}p + \varepsilon,$$

so ist, wenn z eine $\varkappa$te *Stammwurzel* sein soll, also alle Potenzen mit Exponenten e, die $< \varkappa$ sind, *nicht* den Rest 1 geben, ε *nicht* $= 1$, und folglich, da, (46.) in (45.) gesetzt,

$$47. \quad z^{\delta} = \mathfrak{S}p + \varepsilon$$

giebt, in dieser Gleichung ε *nicht* $= 1$. Dieses widerspricht der vorausgesetzten Gleichung: also kann auch für kein $\varkappa$, welches in δ *nicht* aufgeht, z eine $\varkappa$te Stammwurzel sein, sobald (37.) Statt findet.

M. Eben so wenig kann für ein $\varkappa$, welches in $\frac{1}{2}\delta$ *nicht* aufgeht, z eine $\varkappa$te Stammwurzel sein; es sei denn, dafs $\varkappa$ in δ aufginge. Denn setzt man

$$48. \quad \tfrac{1}{2}\delta = n\varkappa + e,$$

wo $e > 0$ und $< \varkappa$, so folgt, ganz wie in (*L.*),

$$49. \quad z^{\frac{1}{2}\delta} = \mathfrak{S}p + \varepsilon.$$

Es müfste also, damit (37.) erfüllt werde, $\varepsilon = -1$ sein können. Dieses kann nun zwar, wenn z eine $\varkappa$te Stammwurzel ist, in

$$50. \quad z^e = \mathfrak{S}p + \varepsilon \ (46.)$$

allerdings der Fall sein, aber nach (1.) nur für $e = \frac{1}{2}\varkappa$; denn nur $z^{\frac{1}{2}\varkappa}$ giebt nach (1.) $\mathfrak{S}p - 1$. Ist nun aber $e = \frac{1}{2}\varkappa$, so ist in (48.)

$$\tfrac{1}{2}\delta = n\varkappa + \tfrac{1}{2}\varkappa \text{ oder}$$

$$51. \quad \delta = n\varkappa + \varkappa,$$

und $\varkappa$ mufs in δ *aufgehen.* Also kann auch für kein $\varkappa$, welches in $\frac{1}{2}\delta$ nicht aufgeht, z eine $\varkappa$te Stammwurzel aus 1 zu p sein; aufser wenn $\varkappa$ in δ aufgeht.

N. Es kommt mithin *nur allein* auf die $\varkappa$ an, *die in δ aufgehen;* nicht auf die $\varkappa$, nach (*K.*), *welche in $\frac{1}{2}\delta$ aufgehen;* und auch auf alle andern nicht.

Ist daher in der Gleichung (6.) für $\varkappa = \frac{1}{2}\delta$, $r = -1$, und für keines der $\varkappa$, welche in δ aufgehen, *ohne* Rücksicht auf diejenigen, welche in $\frac{1}{2}\delta$ aufgehen, weder $r = +1$, noch $r = -1$, so kann z für *keinen* niedrigeren Exponenten als δ eine Stammwurzel aus 1 zu p sein. Für $\varkappa = \delta$ dagegen ist, wegen $z^{\frac{1}{2}\delta} = \mathfrak{S}p - 1$, nothwendig

$$52. \quad z^{\delta} = \mathfrak{S}p + 1;$$

und folglich ist dann z *nothwendig* eine δte Stammwurzel aus 1 zu p; gemäfs (VII.).

O. Ist nicht $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$, sondern

$$53. \quad z^{\frac{1}{2}\delta} = \mathfrak{G}p + r,$$

so ist

$$z^{\delta} = \mathfrak{G}p + r^2,$$

und r^2 ist nun $= +1$ für $r = +1$ oder $r = -1$: also ist dann z^{δ} *nicht* $= \mathfrak{G}p + 1$, und folglich z *nicht* eine δte Stammwurzel.

Werden andrerseits nicht die *übrigen* Bedingungen von (VII.) erfüllt, so ist z ebenfalls *nicht* eine δte Stammwurzel aus 1 zu p, wenn gleich $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$ ist. Also kann nur, wenn *Beides* zugleich Statt findet: nemlich $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$ ist, und die übrigen Bedingungen in (VII.) erfüllt werden, z eine δte Stammwurzel aus 1 zu p sein.

Bew. von VIII. *P.* Geht δ mit 4 auf, so sind δ und $\frac{1}{2}\delta$ beide *gerade.* Für jedes *gerade* δ aber ist nach (1.), wenn z eine δte Stammwurzel aus 1 zu p ist,

$$55. \quad z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1.$$

Nun ist

$$56. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p + (-z)^{\frac{1}{2}\delta}$$

und, da *auch* $\frac{1}{2}\delta$ *gerade* ist,

$$57. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p + z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1 \ (55.).$$

Also *kann* dann $p - z$ eine δte Stammwurzel aus 1 zu p sein; denn (57.) giebt $(p-z)^{\delta} = \mathfrak{G}p + 1$.

Es läfst aber, wenn z eine δte Stammwurzel aus 1 zu p ist, keine *niedrigere* Potenz $z^{\varkappa}$ von z als z^{δ} weder den Rest $+1$, noch, nach (I.), den Rest -1, sondern es ist

$$58. \quad z^{\varkappa} = \mathfrak{G}p + r,$$

wo r *nicht* $+1$ oder -1 ist. Dieses giebt

$$59. \quad (p-z)^{\varkappa} = \mathfrak{G}p + (-z)^{\varkappa} = \mathfrak{G}p \pm r:$$

folglich läfst auch von $p - z$ keine niedrigere als die δte Potenz zu p den Rest 1. Daher ist $p - z$ *nothwendig* eine δte Stammwurzel aus 1 zu p, wenn z eine solche ist; gemäfs (VII. *a.*).

Q. Geht δ mit 2, aber nicht mit 4 auf, so ist δ *gerade* und $\frac{1}{2}\delta$ *ungerade.* Die Gleichung (55.) bleibt dieselbe; aber (56.) giebt jetzt

$$60. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p - z^{\frac{1}{2}\delta} = \mathfrak{G}p + 1 \ (55.):$$

also *kann* jetzt $p - z$ *eine* $\frac{1}{2}\delta$*te* Stammwurzel aus 1 zu p sein. Nun ist in (58.) r für alle $\varkappa < \delta$ nicht $+1$; blofs für $\varkappa = \frac{1}{2}\delta$ ist $r = -1$: also ist jetzt in (59.) r für alle $\varkappa < \delta$ nicht $+1$, und folglich ist $p - z$ *nothwendig* eine $\frac{1}{2}\delta$te Stammwurzel aus 1 zu p; gemäfs (VIII. *b.*).

Bew. von IX. *R. a.* Wenn z_δ eine δte und z_ε eine εte Stammwurzel aus 1 zu p ist, so ist

$$61.\quad z_\delta^\delta = \mathfrak{G}p+1 \text{ und}$$

$$62.\quad z_\varepsilon^\varepsilon = \mathfrak{G}p+1,$$

und keine niedrigere Potenz von z_δ als die δte, und keine niedrigere Potenz von z_ε als die εte giebt zu p den Rest 1.

b. Aus (61.), so wie aus (62.), folgt, wenn man von (61.) die εte und von (62.) die δte Potenz nimmt,

$$63.\quad z_\delta^{\delta\varepsilon} = \mathfrak{G}p+1 \text{ und } z_\varepsilon^{\delta\varepsilon} = \mathfrak{G}p+1,$$

also, Eins mit dem Andern multiplicirt,

$$64.\quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{G}p+1.$$

Daraus folgt, dafs das Product $z_\delta z_\varepsilon$ eine *$\delta\varepsilon$te Stammwurzel* aus 1 zu p sein *kann.*

c. Gesetzt nun, es wäre $z_\delta z_\varepsilon$ schon eine λte Stammwurzel aus 1 zu p, wo $\lambda < \delta\varepsilon$, so dafs schon

$$65.\quad (z_\delta z_\varepsilon)^\lambda = \mathfrak{G}p+1$$

wäre, dann aber keine niedrigere Potenz von $z_\delta z_\varepsilon$ als die λte zu p den Rest 1 gäbe, so müfste λ nothwendig in $\delta\varepsilon$ *aufgehen;* denn wäre es anders und

$$66.\quad \delta\varepsilon = \varkappa\lambda+\varrho,$$

wo $\varrho < \lambda$, so wäre

$$67.\quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = (z_\delta z_\varepsilon)^{\varkappa\lambda+\varrho} = (z_\delta z_\varepsilon)^{\varkappa\lambda}.(z_\delta z_\varepsilon)^\varrho = (\mathfrak{G}p+1)^\varkappa(z_\delta z_\varepsilon)^\varrho \text{ (58.)}$$
$$= \mathfrak{G}p+(z_\delta z_\varepsilon)^\varrho,$$

und da die niedrigere Potenz ϱ als λ von $z_\delta z_\varepsilon$ *nicht* $\mathfrak{G}p+1$ ist, so wäre nach (67.) *nicht* $(z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{G}p+1$. Da dies der Gleichung (63.) widerspricht, so kann in (67. und 66.) ϱ nur Null sein; mithin mufs λ in $\delta\varepsilon$ *aufgehen* und folglich in (66.)

$$68.\quad \delta\varepsilon = \varkappa\lambda$$

sein.

d. Nun lassen *nur* die δ, 2δ, 3δ, ... $\varepsilon\delta$ten Potenzen von z_δ, und *nur* die ε, 2ε, 3ε, ... $\delta\varepsilon$ten Potenzen von z_ε zu p den Rest 1; keine der Potenzen mit *zwischenliegenden* Exponenten. Daraus folgt, dafs für kein Vielfaches, z. B. $\sigma\delta$, von δ, wenn $\sigma < \varepsilon$ ist, für welches nach (61.)

$$69.\quad z_\delta^{\sigma\delta} = \mathfrak{G}p+1$$

ist, *zugleich* in

$$70.\quad z_\varepsilon^{\sigma\delta} = \mathfrak{G}p+e$$

$e=1$ sein kann, sobald δ und ε zu einander *theilerfremd* sind. Denn da

z_ε *nur* mit Exponenten, die Vielfache von ε sind, wie $\tau\varepsilon$, $z^{\tau\varepsilon} = \mathfrak{S}p + 1$ sein kann, so müfste $\sigma\delta = \tau\varepsilon$ sein können; was nur dann der Fall ist, wenn $\sigma = \varepsilon$ und $\tau = \delta$ ist, indem kein Theiler > 1 von ε in δ und kein Theiler > 1 von δ in ε aufgeht, folglich ε *ganz* in σ und τ *ganz* in δ aufgehen mufs.

Es ist also auch, vermöge (69. und 70.), in

$$71.\quad z_\delta^{\sigma\delta} z_\varepsilon^{\sigma\delta} = (z_\delta z_\varepsilon)^{\sigma\delta} = \mathfrak{S}p + e$$

für *kein* $\sigma < \varepsilon$ und auch nicht für ein in ε *aufgehendes* σ, $e = 1$.

e. Auf gleiche Weise folgt, dafs für kein $\sigma < \delta$, auch nicht für ein in δ *aufgehendes* σ, in

$$72.\quad z_\delta^{\sigma\varepsilon} z_\varepsilon^{\sigma\varepsilon} = (z_\delta z_\varepsilon)^{\sigma\varepsilon} = \mathfrak{S}p + e$$

$e = 1$ sein kann.

f. Es kann aber immer $\sigma\delta$ oder $\sigma\varepsilon$ ein *Vielfaches von* λ sein, sobald in (68.) $\varkappa > 1$ ist. Denn vermöge $\varkappa\lambda = \delta\varepsilon$ (68.) mufs $\varkappa$, oder irgend ein Theiler μ von $\varkappa$, in δ oder in ε aufgehen: also ist immer, wenn man $\varkappa = \mu\nu$ setzt,

$$73.\quad \nu\lambda = \frac{\delta}{\mu}\varepsilon \quad \text{oder} \quad = \delta . \frac{\varepsilon}{\mu},$$

wo, nächst ν, $\frac{\delta}{\mu}$ oder $\frac{\varepsilon}{\mu}$ eine *ganze* Zahl ist, die durch σ bezeichnet werden kann. Wäre $\varkappa$ eine Stammzahl oder ohne Theiler, so wäre $\nu = 1$ und $\frac{\delta}{\mu} = \sigma$, oder $\frac{\varepsilon}{\mu} = \sigma$, gleich $\frac{\delta}{\varkappa}$ oder $\frac{\varepsilon}{\varkappa}$.

g. Nun giebt (65.)

$$74.\quad (z_\delta z_\varepsilon)^{\nu\lambda} = (z_\delta z_\varepsilon)^{\sigma\delta} = \mathfrak{S}p + 1 \quad \text{oder}$$

$$75.\quad (z_\delta z_\varepsilon)^{\nu\lambda} = (z_\delta z_\varepsilon)^{\sigma\varepsilon} = \mathfrak{S}p + 1.$$

Diese Gleichungen widersprechen denen (71. und 72.): also kann in (68.) $\varkappa$ nicht > 1 sein. Wenn aber in (71. und 72.) $\sigma = \varepsilon$ oder $= \delta$ ist, so giebt (71. und 72.)

$$76.\quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{S}p + 1 \quad (64.).$$

Dies ist (74. und 75.) gemäfs; wo dann in (73.) $\sigma = \delta$ oder $= \varepsilon$, folglich $\mu = 1$, $\nu = 1$ und $\lambda = \delta\varepsilon$ ist.

Also kann *keine niedrigere* Potenz λ, als $\delta\varepsilon$ selbst, von $z_\delta z_\varepsilon$ zu p den Rest 1 geben; und folglich ist in (74.) das Product $z_\delta z_\varepsilon$ und mithin auch vermöge (7.) r, sobald $r > 1$, *nothwendig* eine $\delta\varepsilon$te Stammwurzel aus 1 zu p, wenn δ und ε zu einander *theilerfremd* sind; gemäfs (IX.).

Bew. von X. *S. a.* Wenn z_δ eine δte Stammwurzel aus 1 zu p ist und man setzt, wie in (8.),

$$77.\quad z_\delta^\varkappa = \mathfrak{G}p + r,$$

so ist, zufolge der Eigenschaft der *Stammwurzeln* für $\varkappa = 1, 2, 3, 4, \ldots \delta - 1$, *r nicht gleich* 1; erst für $\varkappa = \delta$ ist $r = 1$.

b. Ist nun x eine Zahl, von welcher die λte Potenz zu p die δte Stammwurzel z_δ *zum Rest* läfst, so dafs, wie in (9.),

$$78.\quad x^\lambda = \mathfrak{G}p + z_\delta$$

ist, so giebt (77.), wenn man darin aus (78.) $z_\delta = x^\lambda - \mathfrak{G}p$ setzt,

$$79.\quad x^{\varkappa\lambda} = \mathfrak{G}p + r = z_\delta^\varkappa,$$

und folglich ist, vermöge (*a.*), für die Exponenten $\lambda, 2\lambda, 3\lambda, \ldots (\delta-1)\lambda$ von x in (79.) *r nicht gleich* 1.

c. Nun giebt (79.), für eine beliebige Zahl $\mu > 0 < \lambda$,

$$80.\quad x^{\varkappa\lambda+\mu} = \mathfrak{G}p + rx^\mu = z_\delta^\varkappa x^\mu.$$

Käme nun unter den verschiedenen Werthen von r in (77.) irgend ein Rest

$$81.\quad r = x^{\lambda-\mu} - \mathfrak{G}p$$

vor, so wäre in (80.)

$$82.\quad z_\delta^\varkappa x^\mu = \mathfrak{G}p + x^{\lambda-\mu}.x^\mu = \mathfrak{G}p + x^\lambda = \mathfrak{G}p + z_\delta \text{ (78.)}:$$

also müfste, da p nicht durch z_δ theilbar ist, $\mathfrak{G}$ mit z_δ *aufgehen*, und es wäre, wenn man (82.) mit z_δ dividirt,

$$83.\quad z_\delta^{\varkappa-1} x^\mu = \mathfrak{G}p + 1,$$

oder, da $z_\delta = x^{\varkappa\lambda} - \mathfrak{G}p$ ist (79.),

$$84.\quad x^{\varkappa\lambda-\lambda+\mu} = \mathfrak{G}p + 1.$$

d. Es ist aber der Exponent $\varkappa\lambda - (\lambda - \mu) < \delta\lambda$, weil $\mu < \lambda$ und in (77.) $\varkappa < \delta$ ist: also gäbe eine *niedrigere* Potenz von x als $x^{\delta\lambda}$ schon zu p den Rest 1, und folglich wäre dann x *keine* $\lambda\delta$te Stammwurzel aus 1 zu p.

e. Ist dagegen unter den Resten r in (77.) keiner weder $= x^1 - \mathfrak{G}p$, noch $= x^2 - \mathfrak{G}p$, $= x^3 - \mathfrak{G}p, \ldots = x^{\lambda-1} - \mathfrak{G}p$, also auch nicht $= x^{\lambda-\mu} - \mathfrak{G}p$, so ist in (80.) rx^μ *nicht* $= x^\lambda = \mathfrak{G}p + z_\delta$; folglich findet die Gleichung (82.), und mithin diejenige (83.) *nicht* Statt, und folglich ist auch alsdann *keine* niedrigere Potenz von x als $x^{\lambda\delta}$ gleich $\mathfrak{G}p + 1$.

f. Ist $\varkappa = \delta$, so ist in (79.)

$$85.\quad x^{\lambda\delta} = z_\delta^\delta = \mathfrak{G}p + 1,$$

also

$$86.\quad r = 1$$

und folglich in (81.)

$$87.\quad \lambda - \mu = 0$$

und in (83.)

$$88.\quad x^{\lambda\delta} = \mathfrak{G}p + 1;$$

aber keine niedrigere Potenz von x als $x^{\lambda\delta}$ giebt $\mathfrak{G}p+1$. Mithin ist, wenn r weder $=x^1-\mathfrak{G}p$, noch $=x^2-\mathfrak{G}p$, noch $=x^3-\mathfrak{G}p$, ... bis zu $x^{\lambda-1}-\mathfrak{G}p$ ist, x eine $\lambda\delta$te Stammwurzel aus 1 zu p; gemäfs (X.).

§. 67.

Lehrsatz.

I. *Wenn man für eine δte Stammwurzel* z_δ ***aus*** 1 ***zu*** p

$$1.\quad z_\delta^1,\ z_\delta^2,\ z_\delta^3,\ \dots\ z_\delta^{\delta-1},\ z_\delta^\delta = \mathfrak{G}p+(r_1, r_2, r_3, \dots r_{\delta-1}, r_\delta)$$

*setzt, und es ist λ irgend ein **Theiler** von δ, so ist*

$$2.\quad r_1^\lambda+r_2^\lambda+r_3^\lambda+r_4^\lambda+\dots+r_\delta^\lambda=\mathfrak{G}p;$$

*das heifst, die **Summe** der λten Potenzen der Reste* r *in* (1.) *geht mit* p *auf.*

II. *Das **Product** der Reste* r *in* (1.), *mit* p *dividirt, läfst, wenn δ **ungerade** ist,* $+1$, *und wenn δ **gerade** ist,* -1 *zum Rest; das heifst, es ist*

$$3.\quad r_1 r_2 r_3 r_4 \dots r_\delta = \mathfrak{G}p+1, \text{ wenn } \delta \text{ ungerade und}$$

$$4.\quad r_1 r_2 r_3 r_4 \dots r_\delta = \mathfrak{G}p-1, \text{ wenn } \delta \text{ gerade ist.}$$

III. *Zu jeder δten Stammwurzel* z_δ ($\delta=2$ *ausgenommen*) *giebt es eine zweite δte Stammwurzel* x_δ, *und **nur eine**, welche, mit jener multiplicirt und das Product durch* p *dividirt, den Rest* 1 *giebt, so dafs*

$$5.\quad z_\delta . x_\delta = \mathfrak{G}p+1$$

*ist. Die Stammwurzeln sind also immer **zusammengehörige** Zahlen für* 1 *zu* p.

IV. *Das **Product** aller δten Stammwurzeln, für jedes δ, das einzige $\delta=2$ ausgenommen, für welches es nur die einzige Stammwurzel* $p-1$ *giebt, ist* $=\mathfrak{G}p+1$.

Beispiele. (Aus Taf. I.) Zu I. Für die $\delta=12$te Stammwurzel $z_\delta=29$ aus 1 zu p ist die Summe der Reste zu den 1ten, 2ten, 3ten, ... δten Potenzen von $z=29$,

$$6.\quad 29+48+50+47+21+60+32+13+11+14+40+1=366=6.p,$$

und geht also mit p auf.

Ein Theiler λ von δ ist z. B. 4, und die Summe der $\lambda=4$ten Potenzen der Reste (6.) ist, wenn man die Zahlen r in (6.) in der *obersten* horizontalen Zeile der Tafel aufsucht und die zugehörigen Zahlen der *vierten* horizontalen Zeile nimmt,

$$7.\quad 47+13+1+47+13+1+47+13+1+47+13+1=244=4.p.$$

Diese Summe geht also ebenfalls mit p auf; gemäfs (I.).

Zu II. Das *Product* der Reste r in (6.) findet sich wie folgt: $29.48 = \mathfrak{G}p + 50$; $50.50 = -11.-11 = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$; $-1.47 = \mathfrak{G}p - 47 = \mathfrak{G}p + 14$; $14.21 = \mathfrak{G}p + 50$; $50.60 = -11.-1 = \mathfrak{G}p + 11$; $11.32 = \mathfrak{G}p + 47$; $47.13 = \mathfrak{G}p + 1$; $1.11 = \mathfrak{G}p + 11$; $11.14 = \mathfrak{G}p + 32$; $32.40 = \mathfrak{G}p - 1$; $-1.+1 = \mathfrak{G}p - 1$: also ist für das *gerade* $\delta = 12$ das Product der Reste r gleich $\mathfrak{G}p - 1$; gemäfs (4.).

Für das *ungerade* $\delta = 5$ sind z. B. von der 5ten Stammwurzel $z_\delta = 20$ die Reste der 1ten, 2ten, 3ten, 4ten und 5ten Potenz, der Tafel gemäfs, $r = 20, 34, 9, 58$ und 1. Ihr Product ist $20.34 = \mathfrak{G}p + 9$; $9.9 = \mathfrak{G}p + 20$; $20.58 = \mathfrak{G}p + 1$; $1.1 = \mathfrak{G}p + 1$: also ist für das *ungerade* $\delta = 5$ das Product der Reste r gleich $\mathfrak{G}p + 1$; gemäfs (3.).

Zu III. Die $\delta =$ 10ten Stammwurzeln z. B. sind 3, 27, 41 und 52, und es ist $3.41 = 2.p + 1$ und $27.52 = 1404 = 23.p + 1$; gemäfs (III.).

Die $\delta =$ 15ten Stammwurzeln sind 12, 15, 16, 22, 25, 42, 56, 57 und es ist $12.56 = 672 = 11.p + 1$; $15.57 = 855 = 14.p + 1$; $16.42 = 672 = 11.p + 1$ und $22.25 = 550 = 9.p + 1$; gemäfs (III.).

Zu IV. Die $\delta =$ 5ten Stammwurzeln sind 9, 20, 34, 58. Ihr Product ist $9.20 = \mathfrak{G}p - 3$; $-3.34 = \mathfrak{G}p - 41 = \mathfrak{G}p + 20$; $20.58 = -41.-3 = 123 = \mathfrak{G}p + 1$; gemäfs (IV.).

Beweis von I. *A.* Nimmt man von (1.) die Summe der λten Potenzen, so ergiebt sich

8. $$z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + z_\delta^{4\lambda} + \ldots + z_\delta^{\delta\lambda} = \mathfrak{G}p + r_1^\lambda + r_2^\lambda + r_3^\lambda + r_4^\lambda + \ldots + r_\delta^\lambda.$$

Aber es ist, vermöge der Eigenschaft der *Stammwurzeln*,

9. $$z_\delta^\delta = \mathfrak{G}p + 1 \quad \text{und} \quad z_\delta^{\delta\lambda} = \mathfrak{G}p + 1,$$

also, da $z_\delta^\delta = \mathfrak{G}p + r_\delta$ sein soll,

10. $$r_\delta = 1 \quad \text{und} \quad r_\delta^\lambda = 1.$$

Dies in (8.) gesetzt, giebt

11. $$z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + z_\delta^{4\lambda} \ldots + z_\delta^{(\delta-1)\lambda} + \mathfrak{G}p + 1 = r_1^\lambda + r_2^\lambda + r_3^\lambda + r_4^\lambda \ldots + r_{\delta-1}^\lambda + 1.$$

B. Nun ist

12. $$1 + z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + \ldots + z_\delta^{(\delta-1)\lambda} = \frac{z_\delta^{\delta\lambda} - 1}{z_\delta - 1};$$

wie erhellet, wenn man diese Gleichung mit $z_\delta - 1$ multiplicirt.

Aus (9.) ist $z_\delta^\delta - 1 = \mathfrak{G}p$, also $\frac{z_\delta^{\lambda\delta} - 1}{z_\delta - 1} = \frac{\mathfrak{G}p}{z_\delta - 1}$ und es mufs, da p

nicht mit $z_\delta - 1$ aufgeht, $\mathfrak{S}$ mit $z_\delta - 1$ aufgehen und folglich

$$13.\quad \frac{z_\delta^{\lambda\delta}-1}{z_\delta-1} = \mathfrak{S}p$$

sein.

C. Dieses giebt in (12.)

$$14.\quad 1+z_\delta^\lambda+z_\delta^{2\lambda}+z_\delta^{3\lambda}+\ldots+z_\delta^{(\delta-1)\lambda} = \mathfrak{S}p$$

und in (11.) $\mathfrak{S}p+\mathfrak{S}p = r_1^\lambda+r_2^\lambda+r_3^\lambda+\ldots+r_{\delta-1}^\lambda+1$, oder, da $1=r_\delta^\lambda$ ist (10.),

$$15.\quad r_1^\lambda+r_2^\lambda+r_3^\lambda+r_4^\lambda+\ldots+r_{\delta-1}^\lambda+r_\delta^\lambda = \mathfrak{S}p;$$

wie (1.).

Bew. von II. *D.* Multiplicirt man die Gleichungen (1.) mit einander, so ergiebt sich

$$16.\quad z_\delta^{1+2+3+4+\ldots+\delta-1}.z_\delta^\delta = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta$$

oder, da $z_\delta^\delta = \mathfrak{S}p+1$ (9.) ist,

$$17.\quad z_\delta^{1+2+3+4+\ldots+\delta-1} = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta$$

oder

$$18.\quad z_\delta^{\frac{1}{2}\delta(\delta-1)} = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta.$$

a. Ist nun δ *ungerade*, also $\delta-1$ *gerade*, so giebt (18.), wegen $z_\delta^\delta = \mathfrak{S}p+1$ (9.), $(\mathfrak{S}p+1)^{\frac{1}{2}(\delta-1)} = \mathfrak{S}p+r_1r_2r_3\ldots r_\delta$ oder

$$19.\quad r_1r_2r_3\ldots r_\delta = \mathfrak{S}p+1;$$

gemäfs (3.).

b. Ist δ *gerade*, also $\delta-1$ *ungerade*, so ist $z_\delta^{\frac{1}{2}\delta} = \mathfrak{S}p-1$ (§. 66. I.); also giebt dann (18.) $(\mathfrak{S}p-1)^{\delta-1} = \mathfrak{S}p+r_1r_2r_3\ldots r_\delta$ und, da $\delta-1$ ungerade ist,

$$20.\quad r_1r_2r_3\ldots r_\delta = \mathfrak{S}p-1;$$

gemäfs (4.).

Bew. von III. *E.* Gemäfs (§. 47. I.) giebt es zu jeder der Zahlen

$$21.\quad z = 2, 3, 4, 5, \ldots p-1$$

eine zweite, von z_1 *verschiedene* Zahl z_2 aus derselben Reihe, und *nur eine*, für welche

$$22.\quad z_1z_2 = \mathfrak{S}p+1$$

ist.

F. (22.) giebt für *jeden* beliebigen Exponenten $\varkappa$

$$23.\quad z_1^\varkappa z_2^\varkappa = \mathfrak{S}p+1.$$

Ist nun z_1 eine δte Stammwurzel aus 1 zu p, so ist vermöge ihrer Eigenschaften, wenn man

$$24.\quad z_1^\varkappa = \mathfrak{S}p+e$$

setzt, e für $\varkappa = 1, 2, 3, 4, \ldots \delta-1$ *nicht* $=1$, für $\varkappa=\delta$ aber *nothwendig* $=1$.

G. Setzt man andrerseits

$$25.\quad z_2^\varkappa = \mathfrak{G}p + \varepsilon,$$

so ist aus (24. und 25.)

$$26.\quad z_1^\varkappa z_2^\varkappa = (\mathfrak{G}p + e)(\mathfrak{G}p + \varepsilon) = \mathfrak{G}p + e\varepsilon$$

und vermöge (23.)

$$27.\quad e\varepsilon = \mathfrak{G}p + 1.$$

H. Da nun nach (*F.*) e für $\varkappa = 1, 2, 3, 4, \ldots \delta - 1$ *nicht* $= 1$ ist, so kann auch gemäfs (27.) ε für $\varkappa = 1, 2, 3, 4, \ldots \delta - 1$ *nicht* $= 1$ sein; denn wäre $\varepsilon = 1$ für eines dieser $\varkappa$, so wäre $e\varepsilon$ nicht $= \mathfrak{G}p + 1$, wie es sein soll, sondern $= \mathfrak{G}p + e$.

Da ferner nach (*F.*) für $\varkappa = \delta$, e nothwendig $= 1$ ist, so ist auch vermöge (27.) für $\varkappa = \delta$, ε nothwendig $= 1$; denn wäre ε nicht $= 1$, so wäre nicht $e\varepsilon = \mathfrak{G}p + 1$, wie es sein soll, sondern $= \mathfrak{G}p + \varepsilon$.

I. Es mufs also in (25.) für $\varkappa = 1, 2, 3, 4, \ldots \delta - 1$, ε *nicht* $= 1$ und für $\varkappa = \delta$, ε *gleich* 1 sein, und deshalb ist z_2 nothwendig eine δte Stammwurzel, wenn z_1 eine solche ist. Mithin giebt es nothwendig zu jeder δten Stammwurzel $z_1 = z_\delta$ eine zweite $z_2 = x_\delta$, welche, mit jener multiplicirt und das Product durch p dividirt, den Rest 1 giebt.

K. Und zwar giebt es *nur eine* solche: denn gäbe es eine zweite z_3, für welche

$$28.\quad z_1 z_3 = \mathfrak{G}p + 1$$

wäre, so wäre

$$29.\quad \text{aus (22.)}\quad z_1 z_2 z_3 = \mathfrak{G}p + z_3$$

$$30.\quad \text{und aus (28.)}\quad z_1 z_2 z_3 = \mathfrak{G}p + z_2.$$

Da (29.) und (30.) sich widersprechen, wenn nicht $z_2 = z_3$ ist, so kann es keine zweite zu z_1 gehörige Stammwurzel geben.

Dieses zusammen ist was (III.) behauptet und es folgt, dafs die Stammwurzeln *zusammengehörige Zahlen* für 1 zu p sind.

Bew. von IV. ***L.*** Wenn z_δ eine der δten Stammwurzeln aus 1 zu p ist und man setzt

$$31.\quad z_\delta^\varkappa = \mathfrak{G}p + r_\varkappa,$$

so sind nach (§. 60. II.) die Reste r für diejenigen Exponenten $\varkappa$, welche zu δ *theilerfremd* sind, *alle die δten Stammwurzeln* z_δ selbst.

Bezeichnet man also die zu δ *theilerfremden* $\varkappa$ durch $\varkappa_1, \varkappa_2, \varkappa_3, \ldots$ und die in (31.) zugehörigen ***Reste*** durch $r_1, r_2, r_3, \ldots$, so dafs für ***irgend eine*** der δten Stammwurzeln z_δ

$$32.\quad \begin{cases} z_\delta^{\varkappa_1} = \mathfrak{S}p + r_1, \\ z_\delta^{\varkappa_2} = \mathfrak{S}p + r_2, \\ z_\delta^{\varkappa_3} = \mathfrak{S}p + r_3, \\ \ldots\ldots\ldots\ldots \end{cases}$$

ist, so sind die r in (32.) alle die δten Stammwurzeln z_δ selbst.

M. Multiplicirt man nun die Gleichungen (32.) mit einander, so ergiebt sich

$$33.\quad z_\delta^{\varkappa_1+\varkappa_2+\varkappa_3+\varkappa_4+\ldots} = \mathfrak{S}p + r_1 r_2 r_3 r_4 \ldots$$

Nun *geht* aber nach (§. 65. II.) die Summe $\varkappa_1 + \varkappa_2 + \varkappa_3 + \varkappa_4 \ldots$, aller zu der Zahl δ theilerfremden Zahlen, $\delta = 2$ ausgenommen, mit δ *auf,* also giebt (33.)

$$34.\quad z_\delta^{\mathfrak{S}\delta} = \mathfrak{S}p + r_1 r_2 r_3 r_4 \ldots,$$

und da vermöge der Eigenschaft der Stammwurzeln $z_\delta^\delta = \mathfrak{S}p + 1$, also auch $z_\delta^{\mathfrak{S}\delta} = \mathfrak{S}p + 1$ ist, so giebt (34.)

$$35.\quad r_1 r_2 r_3 r_4 \ldots = \mathfrak{S}p + 1;$$

das heifst: das Product aller δten Stammwurzeln $r_1, r_2, r_3, r_4, \ldots$ aus 1 zu p ist $= \mathfrak{S}p + 1$. $\delta = 2$ ist ausgenommen, für welches δ es *nur die eine* Stammwurzel $p - 1$ giebt.

Anm. *N.* Immer, wenn bewiesen werden soll, dafs z z. B. eine δte *Stammwurzel* aus 1 zu der Stammzahl p sei, ist nicht zu übersehen, dafs deshalb, weil etwa sich findet, die δte Potenz von z durch p dividirt lasse den Rest 1, das heifst, die Gleichung $z^\delta = \mathfrak{S}p + 1$ werde erfüllt, z noch keineswegs *nothwendig* eine δte Stammwurzel aus 1 zu p sei. Es mufs vielmehr immer noch besonders bewiesen werden, dafs keine *niedrigere* als die δte Potenz von z, durch p dividirt, den Rest 1 läfst; denn dies ist die *zweite* Bedingung für *Stammwurzeln.*

§. 68.

Lehrsatz.

I. -3 *ist Quadratrest zu allen Stammzahlen* $p = 6n + 1$ *und Nichtquadratrest zu allen Stammzahlen* $p = 6n - 1$.

II. $+3$ *ist Quadratrest zu allen Stammzahlen* $p = 12n + 1$ *und* $12n - 1$ *und Nichtquadratrest zu allen Stammzahlen* $p = 12n + 5$ *und* $12n - 5$.

III. *Setzt man für die Stammzahlen* $p = 6n + 1$

$$1.\quad z^2 = \mathfrak{S}p - 3,$$

wo z *die beiden Werthe* z *und* p — z *hat, so sind die beiden dritten Stammwurzeln* x_3 *aus* 1 *zu* p:

2. $x_3 = \frac{1}{2}(z-1)$ *oder* $\frac{1}{2}(p-z-1)$ *und*

3. $x_3 = p - \frac{1}{2}(z+1)$ *oder* $\frac{1}{2}(p+z-1)$.

IV. *Die beiden sechsten Stammwurzeln* x_6 *aus* 1 *zu* p *sind um* 1 *gröfser, also*

4. $x_6 = \frac{1}{2}(z+1)$ *oder* $\frac{1}{2}(p-z+1)$ *und*

5. $x_6 = p - \frac{1}{2}(z-1)$ *oder* $\frac{1}{2}(p+z+1)$.

Beispiele. Zu I. und III. Wie aus der am Ende dieses Bandes angehängten Tafel zu ersehen, ist

6.
1. -3 *Quadratrest* zu $p =$ 5 7 13 19 31 37 43 61 67 73 79 97 $= 6n+1$,
2. und *Nichtquadratrest* zu $p =$ 11 17 23 29 41 47 53 59 71 83 89 101 $= 6n-1$,
3. $+3$ ist *Quadratrest* zu $p =$ 11 13 23 37 47 59 61 71 73 83 97 $= 12n \pm 1$,
4. und *Nichtquadratrest* zu $p =$ 5 7 17 19 29 31 41 43 53 67 79 89 101 $= 12n \pm 5$.

Zu III. 1. Nach Taf. I. ist $27^2 = \mathfrak{G}p + 58 = \mathfrak{G}p - 3$ und $34^2 = \mathfrak{G}p + 58 = \mathfrak{G}p - 3$, also hat für $p = 61 = 6n+1$, z in (1.) die beiden Werthe 27 und 34. $z = 27$ giebt nach (2. und 3.) $x_3 = \frac{1}{2}(27-1) = 13$ und $x_3 = 61 - \frac{1}{2}(27+1) = 61 - 14 = 47$; $z = 34$ giebt ebenfalls $x_3 = \frac{1}{2}(61-34-1) = 13$ und $x_3 = \frac{1}{2}(61+34-1) = 47$, und 13 und 47 sind, wie die Tafel zeigt, die beiden *dritten* Stammwurzeln aus 1 zu p. Die beiden *sechsten* Stammwurzeln aus 1 zu p, der Tafel nach 14 und 48, sind *um* 1 *gröfser.*

2. Für $p = 43$ ist $13^2 = \mathfrak{G}p + 40 = \mathfrak{G}p - 4$ und $30^2 = \mathfrak{G}p + 40 = \mathfrak{G}p - 3$; also hat hier z in (1.) die beiden Werthe 13 und 30. $z = 13$ giebt nach (2. und 3.) $x_3 = \frac{1}{2}(13-1) = 6$ und $x_3 = 43 - \frac{1}{2}(13+1) = 43 - 7 = 36$, und $z = 30$ giebt $x_3 = \frac{1}{2}(43-30-1) = 6$ und $x_3 = \frac{1}{2}(43+30-1) = 36$, und 6 und 36 sind die beiden *dritten* Stammwurzeln aus 1 zu p. Die beiden *sechsten* Stammwurzeln aus 1 zu p sind 7 und 37, also um 1 gröfser.

Beweis. *A.* Für die dritten *Stammwurzeln* aus 1 zu p ist

7. $x^3 = \mathfrak{G}p + 1$.

Von den *drei* ganzzahligen Werthen > 0 und $< p$, welche x für diese Gleichung nach (§. 54.) haben *kann* und von welchen $x = 1$ einer ist, sind nothwendig die beiden andern, > 1, *dritte Stammwurzeln* aus 1 zu p, weil die *zwei* Zahlen 1 und 2 mit 3 keinen Theiler > 1 gemein haben und also nach (§. 63. I.) *zwei* Stammwurzeln, folglich *zwei* Werthe von $x > 1$ Statt finden müssen, die der Gleichung (7.) genugthun, und die also die *beiden andern* ganzzahligen Wurzeln der Gleichung (7.) sind, welche es *aufser* $x = 1$ geben kann und hier also geben *mufs.*

B. Die beiden Wurzeln, >1, von der Gleichung (7.) sind diejenigen der Gleichung

$$8. \quad x^2+x+1 = \mathfrak{S}p;$$

denn (7.) giebt

$$9. \quad x^3-1 = (x-1)(x^2+x+1) = \mathfrak{S}p,$$

und dieser Gleichung wird zunächst durch $x=1$ und dann durch die beiden Werthe, welche x in (8.) haben kann, entsprochen.

C. Löset man nun die quadratische Gleichung (8.) auf die gewöhnliche Weise auf, so ergiebt sich $x = -\frac{1}{2}\pm\sqrt{(\frac{1}{4}-1+\mathfrak{S}p)}$ oder

$$10. \quad x = \frac{-1\pm\sqrt{(\mathfrak{S}p-3)}}{2}.$$

Diese beiden Werthe von x, welche (10.) ausdrückt, sind also die beiden *dritten Stammwurzeln* >1 aus 1 zu p.

D. Geht nun $p-1$ mit 3 auf, und mithin, da $p-1$ *immer gerade* ist und folglich *zugleich* mit 2 aufgeht, mit 6 (§. 26.), so dafs p von der Form $p=6n+1$ ist, so giebt es *nothwendig* ganzzahlige dritte Stammwurzeln aus 1 zu p; denn es giebt deren nach (§. 58. I.) für *jeden* Theiler δ von $p-1$, also hier auch für $\delta=3$. Daraus folgt, dafs der Ausdruck in (10.) von x *ganze Zahlen* geben *mufs*.

E. Dieses aber ist nicht anders möglich, als wenn $\mathfrak{S}p-3$ ein *Quadrat* und folglich -3 ein *Quadratrest* zu p ist. Denn wäre $\mathfrak{S}p-3$ *nicht* ein Quadrat, für kein $\mathfrak{S}$, so wäre $\mathfrak{S}p-3$ eine *irrationale* und folglich x keine *ganze* Zahl. Also *mufs* nothwendig nach (1.)

$$11. \quad z^2 = \mathfrak{S}p-3$$

und also in (10.)

$$12. \quad x = \frac{-1\pm z}{2}$$

sein.

F. Mehr, als dafs $\mathfrak{S}p-3$ ein Quadrat z sei, ist aber auch in (10.) nicht nöthig, um die beiden Werthe von x zu *ganzen* Zahlen zu machen. Denn der Gleichung (11.) thut auch ebensowohl $p-z$ als z ein Genüge; also ist auch in (10.), ebensowohl wie in (12.), $x=\frac{-1\pm z}{2}$ ist, auch

$$13. \quad x = \frac{-1\pm(p-z)}{2}.$$

Ist nun z *ungerade*, so sind in (12.) $z-1$ und $-z-1=-(z+1)$ beide *gerade*, und folglich sind x zwei ganze Zahlen. Ist z *gerade*, so ist $p-z$ *ungerade*, und es folgt auf dieselbe Weise, dafs dann die x in (13.)

zwei ganze Zahlen sind. Es gilt (12.) für den *ungeraden*, (13.) für den *geraden* Werth von z; und so geben denn auch die beiden Gleichungen (12. und 13.) nicht etwa *vier* verschiedene Werthe von x, sondern nur *dieselben zwei* Werthe. Denn ist in (12.) z *ungerade*, so mufs man für (13.) den *geraden* Werth von z nehmen, welcher $p-z$ ist, und dadurch reducirt sich (13.) auf $x=\frac{-1\pm(p-(p-z))}{2}=\frac{-1\pm z}{2}$, welches *Dasselbe* wie (12.) ist. Ist in (13.) z *gerade*, so mufs man für (12.) den andern, *ungeraden* Werth von z setzen, welcher $p-z$ ist, damit *so* alle verschiedenen Werthe in Rechnung kommen; und dadurch reducirt sich (12.) auf $x=\frac{-1\pm(p-z)}{2}$; welches Dasselbe wie (13.) ist.

Bis hierher folgt also, dafs für Stammzahlen $p=6n+1$, -3 nothwendig *Quadratrest* sein mufs und dafs dann

$$14.\quad x_3=\tfrac{1}{2}(z-1) \text{ oder } \tfrac{1}{2}(p-z-1)$$

und $x_3=-\frac{1}{2}(z+1)$ oder $-\frac{1}{2}(p-z+1)$, oder, was dasselbe ist,

$$15.\quad x_3=p-\tfrac{1}{2}(z+1) \text{ oder } p-\tfrac{1}{2}(p-z+1)=\tfrac{1}{2}(p+z-1)$$

die beiden dritten Stammwurzeln aus 1 zu p sind; wie es (I.) und (III.) behauptet.

G. Ferner sind die 6ten Stammwurzeln x_6, aus 1 zu p, da 3 eine *Stammzahl* ist, nach (§. 66. VI.) $=p-z$. Man findet sie also, wenn man die x_3 (2. und 3.) von p abzieht. Dieses giebt die Ausdrücke (IV. 4. und 5.) von x_6. Die sechsten Stammwurzeln aus 1 zu p sind, wie (4. und 5.) zeigen, um 1 gröfser als die dritten.

H. Ist p von der Form $6n-1$, so geht $p-1=6n-2$ *nicht* mit 3 auf, und folglich giebt es für $p=6n-1$ *keine* dritten Stammwurzeln aus 1 zu p. Es gäbe aber dergleichen vermöge (10.), wenn -3 auch für die Stammzahlen $p=6n-1$ *Quadratrest* wäre. Also kann -3 für solche Stammzahlen *kein* Quadratrest sein. Und da nun *jede* Zahl entweder Quadratrest oder Nichtquadratrest ist, so ist -3 für alle Stammzahlen $p=6n-1$ nothwendig *Nichtquadratrest;* gemäfs (I.).

I. a. Nach (§. 50. I.) sind für Stammzahlen $p=4n+1$, für welche also $p-1$ mit 4 aufgeht, die *zeichenfreien* Werthe der positiven und der negativen *Quadratreste dieselben.* Nun ist -3 Quadratrest zu den Stammzahlen $p=6n+1$ (I.), für welche $p-1$ mit 6 aufgeht. Geht also $p-1$ mit 4 und mit 6 *zugleich* auf, so ist auch $+3$ *Quadratrest* zu p. Jenes ist der Fall für $p=12n+1$; also ist zu den Stammzahlen $p=12n+1$, $+3$ *Quadratrest;* gemäfs (II.).

b. Eben so sind nach (§. 50. I.) für Stammzahlen $p=4n+1$, für welche also $p-1$ mit 4 aufgeht, die ***zeichenfreien*** Werthe der positiven und der negativen ***Nichtquadratreste*** dieselben. Nun ist -3 Nichtquadratrest zu den Stammzahlen $p=6n-1$ (I.), für welche $p+1$ mit 6 aufgeht. Geht also $p-1$ mit 4 und zugleich $p+1$ mit 6 auf, so ist auch $+3$ ***Nichtquadratrest*** zu p. Jenes ist der Fall für $p=12n+5$: also ist zu den Stammzahlen $p=12n+5$, $+3$ ***Nichtquadratrest;*** gemäfs (II.).

c. Nach (§. 50. II.) sind für die Stammzahlen $p=4n-1$, für welche $p+1$ mit 4 aufgeht, die zeichenfreien Werthe der negativen ***Nichtquadratreste*** die positiven ***Quadratreste.*** Nun ist nach (I.) -3 ***Nichtquadratrest*** zu den Stammzahlen $p=6n-1$, für welche $p+1$ mit 6 aufgeht. Geht also $p-1$ mit 4 und mit 6 ***zugleich*** auf, so ist $+3$ ***Quadratrest*** zu p. Jenes ist der Fall für $p=12n-1$: also ist zu den Stammzahlen $p=12n-1$, $+3$ ***Quadratrest;*** gemäfs (II.).

d. Endlich sind nach (§. 50. II.) für die Stammzahlen $p=4n-1$, für welche $p+1$ mit 4 aufgeht, die zeichenfreien Werthe der negativen ***Quadratreste*** die positiven ***Nichtquadratreste.*** Nun ist nach (I.) -3 ***Quadratrest*** zu den Stammzahlen $p=6n+1$, für welche also $p-1$ mit 6 aufgeht. Geht also $p+1$ mit 4 und ***zugleich*** $p-1$ mit 6 auf, so ist $+3$ ***Nichtquadratrest*** zu p. Jenes ist der Fall für $p=12n-5$: also ist zu den Stammzahlen $p=12n-5$, $+3$ ***Nichtquadratrest;*** gemäfs (II.).

Zweiter Beweis von I. und II. ***K.*** Nach dem ***Gegenseitigkeitsgesetze für Quadratreste*** (§. 49. II.) sind zwei Stammzahlen p und q zu einander ***zugleich*** positiver Quadratrest oder positiver Nichtquadratrest, wenn p und q nicht beide von der Form $4n-1$ sind; und zugleich positiver Quadratrest und positiver Nichtquadratrest, oder umgekehrt, wenn ***beide*** von der Form $4n-1$ sind. Nach (49. I.) aber ist, wenn z. B. p ***Quadratrest*** zu q ist, also in (§. 49. 1.) die Stelle von r einnimmt,

$$16. \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1,$$

und wenn p ***Nichtquadratrest*** zu q ist, also in (§. 49. 2.) die Stelle von ϱ einnimmt,

$$17. \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1.$$

Also im Fall p und q ***nicht beide*** von der Form $4n-1$ sind, ist nach dem Gegenseitigkeitsgesetz:

$$18. \quad \textit{Zugleich} \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1 \quad \text{und} \quad q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1 \quad \text{und}$$

$$19. \quad \textit{Zugleich} \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1 \quad \text{und} \quad q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1.$$

Sind p und q *beide* von der Form $4n-1$, so ist

20. *Zugleich* $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1$ und $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ und

21. *Zugleich* $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1$ und $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$.

L. Nun ist die Zahl 3, von welcher man wissen will, zu welchen Stammzahlen p sie Quadratrest oder Nichtquadratrest sei, ebenfalls eine *Stammzahl:* es gilt also von ihr, p gegenüber, das Gegenseitigkeitsgesetz und man kann sie *statt* q setzen. Dieses giebt

a. In (18.)

$$22. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3+1:$$

also, wenn zunächst p von der Form $3\mathfrak{G}+1$ oder $3n+1$ ist, so ist nach (18.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, und folglich ist nach (§. 49. 1.) $+3$ *Quadratrest* zu p. Aber es kommt für (18.) zugleich darauf an, dafs p und q *nicht beide* von der Form $4n-1$ sind. Hier ist $3=q$ von der Form $4n-1$, also gilt (18.) nur, wenn p von der Form $4n+1$ ist. Mithin mufs p *zugleich* von der Form $3n+1$ und von der Form $4n+1$ sein, folglich von der Form $12n+1$, wenn $+3$ *Quadratrest* zu p sein soll.

b. Setzt man in (19.) 3 statt q, so ergiebt sich

$$23. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3-1:$$

also, wenn zunächst p von der Form $3\mathfrak{G}-1$ oder $3n-1$ ist, so ist nach (19.) zugleich $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ und folglich $+3$ nach (§. 49. 2.) *Nichtquadratrest* zu p. Aber es mufs wieder, wie vorhin, p *zugleich* von der Form $4n+1$ sein, weil $q=3$ von der Form $4n-1$ ist und, wenn (19.) Statt finden soll, p und q *nicht beide* von der Form $4n-1$ sein dürfen. Also mufs p von der Form $3n-1$ und zugleich von der Form $4n+1$, also von der Form $12n+5$ sein, wenn $+3$ *Nichtquadratrest* zu p sein soll; denn zu $12n+5$, 1 addirt, geht mit 3, und 1 davon abgezogen, geht mit 4 auf.

c. Setzt man 3 statt q in (20.), so ergiebt sich

$$24. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3+1,$$

also, wenn zunächst p von der Form $3n+1$ ist, so ist nach (20.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$, also nach (§. 49. 2.) $+3$ *Nichtquadratrest* zu p; aber nur insofern p zugleich, eben wie $q=3$, von der Form $4n-1$ ist; der Bedingung für (20.) gemäfs. Wenn also p von der Form $3n+1$ und $4n-1$ *zugleich* ist, so ist $+3$ *Nichtquadratrest* zu p. Dieses giebt die Form $12n-5$; denn 1 davon abgezogen geht mit 3, und 1 dazu addirt, mit 4 auf.

d. Setzt man endlich 3 statt q in (21.), so ergiebt sich

$$25. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3-1,$$

also, wenn zunächst p von der Form $3n-1$ ist, so ist nach (21.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, also nach (§. 49. 1.) $+3$ *Quadratrest* zu p; aber nur insofern p zugleich, eben wie $q=3$, von der Form $4n-1$ ist; der Bedingung für (21.) gemäfs. Wenn also p von der Form $3n-1$ und $4n-1$ *zugleich* ist, so ist $+3$ *Quadratrest* zu p. Dieses giebt die Form $12n-1$; denn, 1 dazu addirt, geht mit 3 und mit 4 auf.

e. **Zusammen** also ist nach (*a.* und *d.*) und nach (*b.* und *c.*)

26. $+3$ *Quadratrest* zu p, wenn p von der Form $12n+1$ oder $12n-1$ ist und

27. $+3$ *Nichtquadratrest* zu p, wenn p von der Form $12n+5$ oder $12n-5$ ist;

gemäfs (II.).

M. Zu welchen Stammzahlen p, -3 Quadratrest oder Nichtquadratrest sei, kann man auf den Grund dessen, was so eben für $+3$ gefunden worden ist, aus dem Lehrsatze (§. 50.) abnehmen.

a. Nemlich, nach (§. 50. I.) sind die *zeichenfreien* Werthe der positiven und negativen echten Quadratreste und Nichtquadratreste für alle Stammzahlen $p=4n+1$ *dieselben.* Von der Form $4n+1$ sind in (26. und 27.) die Formen $12n+1$ und $12n+5$. Also ist zu $p=12n+1$, eben wie $+3$, auch -3 *Quadratrest,* und zu $p=12n+5$, eben wie $+3$, auch -3 *Nichtquadratrest.*

b. Nach (§. 50. II.) geben für alle Stammzahlen $p=4n-1$ die positiven Quadratreste die zeichenfreien Werthe der negativen Nichtquadratreste und die positiven Nichtquadratreste die zeichenfreien Werthe der negativen Quadratreste. Von der Form $4n-1$ sind in (26. und 27.) die Formen $12n-1$ und $12n-5$. Also ist zu $p=12n-1$, -3 *Nichtquadratrest* und zu $p=12n-5$, -3 *Quadratrest.*

c. Zusammen also ist zufolge (*a.* und *b.*) -3 *Quadratrest* zu $p=12n+1$ und zu $p=12n-5$, und *Nichtquadratrest* zu $p=12n+5$ und $p=12n-1$. Die Form $6n+1$ drückt, wenn man $2n$ und $2n-1$ statt n setzt, $12n+1$ und $6(2n-1)+1=12n-1$ *zugleich* aus. Eben so drückt die Form $6n-1$, wenn man $2n+1$ und $2n$ statt n setzt, $6(2n+1)-1 = 12n-5$ und $12n-1$ *zugleich* aus. Also ist, kürzer:

28. -3 *Quadratrest* zu p, wenn p von der Form $6n+1$ ist und

29. -3 *Nichtquadratrest* zu p, wenn p die Form $6n-1$ hat;

gemäfs (I.).

Man kann indessen die Resultate für -3 auch wie folgt direct aus dem Gegenseitigkeitsgesetz entnehmen.

N. Da $q=3$ von der Form $4n-3$ ist, so gelten (18. und 19.) ***nur*** für $p=4n+1$, und (20. und 21.) ***nur*** für $p=4n-1$.

a. Ist nun $p=4n+1$, so ist $\frac{1}{2}(p-1)=\frac{1}{2}.4n=2n$ eine ***gerade*** Zahl, also ist $(-3)^{\frac{1}{2}(p-1)}=(+3)^{\frac{1}{2}(p-1)}$. Für die p, welche ***die Form*** $4n+1$ ***haben***, kann man also -3 statt $+3$ setzen: also zu allen den $p=4n+1$, zu welchen $+3$ Quadratrest oder Nichtquadratrest ist, ist es auch -3. In (***L. a.***) ist $p=4n+1$, und $+3$ ist ***Quadratrest*** zu $p=12n+1$, also ist auch -3 ***Quadratrest*** zu $p=12n+1$.

In (***L. b.***) ist $p=4n+1$ und $+3$ ***Nichtquadratrest*** zu $p=12n+5$, also ist auch -3 Nichtquadratrest zu $p=12n+5$.

b. Ist $p=4n-1$, so ist $\frac{1}{2}(p-1)=\frac{1}{2}(4n-2)=2n-1$ eine ***ungerade*** Zahl, also ist $(-3)^{\frac{1}{2}(p-1)}=-(+3)^{\frac{1}{2}(p-1)}$, und folglich ist, wenn $(+3)^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$ ist, $(-3)^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$; und umgekehrt. Zu allen $p=4n-1$ also, zu welchen $+3$ Quadratrest ist, ist -3 Nichtquadratrest; und umgekehrt.

In (***L. c.***) ist $p=4n-1$, und $+3$ ist ***Nichtquadratrest*** zu $p=12n-5$; also ist -3 ***Quadratrest*** zu $p=12n-5$.

In (***L. d.***) ist $p=4n-1$, und $+3$ ist ***Quadratrest*** zu $p=12n-1$; also ist -3 ***Nichtquadratrest*** zu $p=12n-1$.

c. Zusammen also ist hier nach (***a.*** und ***b.***) -3 ***Quadratrest*** zu $p=12n+1$ und $p=12n-5$ und ***Nichtquadratrest*** zu $p=12n+5$ und $p=12n-1$; eben wie in (***M. c.***).

Anm. ***O.*** In (***B.*** und ***C.***) kommt eine Anwendung der Auflösung einer gewöhnlichen algebraischen Gleichung auf einen Zahlensatz vor; in dem zweiten Beweise eine Anwendung des Gegenseitigkeitsgesetzes.

§. 69.

Lehrsatz.

I. $+5$ ***ist Quadratrest zu allen Stammzahlen*** $\mathrm{p}=10\mathrm{n}+1$; ***jedoch nicht zu diesen allein. Es ist also, wenn man***

$$1. \quad \mathrm{z}^2=\mathfrak{G}\mathrm{p}+5$$

setzt, wo z ***die zwei Werthe*** z ***und*** p$-$z ***oder*** $+$z ***und*** $-$z ***hat,*** z ***eine ganze Zahl*** $>0<\mathrm{p}-1$.

II. ***Ferner ist dann auch für die beiden Werthe von*** z ***in*** (1.)

$$2. \quad 2\mathrm{z}-10 \textit{ Quadratrest zu } \mathrm{p}, \textit{ für } \mathrm{p}=10\mathrm{n}+1,$$

nicht aber für andere Stammzahlen; so daſs also, wenn man für die beiden Werthe von z, ***hier für*** $\mathrm{p}=10\mathrm{n}+1$,

$$3.\quad y^2 = \mathfrak{S}p + 2z - 10$$

setzt, wo y *wiederum zwei Werthe* y *und* p—y *oder* +y *und* —y *hat, für jeden der beiden Werthe von* z, *also zusammen* **vier** *Werthe, auch* y *eine* **ganze** *Zahl* > 0 *und* < p — 1 *ist.*

III. ***Die vier fünften Stammwurzeln*** *aus* 1 *zu* p *sind*

$$4.\quad x_5 = \frac{\mathfrak{S}p - 1 + z + y}{4},$$

wenn man jeden der beiden Werthe von z *in* (1.) *je mit den beiden zu den* **andern** *Werthen von* z *gehörigen zwei Werthen von* y *in* (3.) *verbindet.*

IV. ***Die vier zehnten Stammwurzeln*** *aus* 1 *zu* p *sind*

$$5.\quad x_{10} = p - x_5.$$

Beispiel. Es sei $p = 61$, so ist nach Taf. I. für (1.):

$$6.\quad z = +26 \text{ und } +35 = p - 26, \text{ also } z = +26 \text{ und } -26.$$

Dieses giebt in (3.), Taf. I. zufolge,

$$7.\quad y^2 = \mathfrak{S}p + 2.26 - 10 = \mathfrak{S}p + 42, \text{ also } y = 15 \text{ und } 46 = p - 15 \text{ oder } y = +15 \text{ und } -15 \text{ für } z = +26, \text{ und}$$

$$8.\quad y^2 = \mathfrak{S}p - 2.26 - 10 = \mathfrak{S}p + 60, \text{ also } y = 11 \text{ und } 50 = p - 11 \text{ oder } y = +11 \text{ und } -11 \text{ für } z = -26.$$

Die beiden Werthe von y für den Werth $+26$ von z sind also $+15$ und -15, und die beiden Werthe von y für den Werth -26 von z sind $+11$ und -11.

Dieses giebt zufolge (III.) für die vier Werthe von x_5:

$$9.\ \begin{cases} 1.\quad x_5 = \dfrac{\mathfrak{S}p - 1 + 26 + 11}{4} = \dfrac{\mathfrak{S}p + 36}{4} = 9, \\ 2.\quad x_5 = \dfrac{\mathfrak{S}p - 1 + 26 - 11}{4} = \dfrac{\mathfrak{S}p + 14}{4} = \dfrac{2.61 + 14}{4} = \dfrac{136}{4} = 34; \\ 3.\quad x_5 = \dfrac{\mathfrak{S}p - 1 - 26 + 15}{4} = \dfrac{\mathfrak{S}p - 12}{4} = \dfrac{4.61 - 12}{4} = \dfrac{232}{4} = 58; \\ 4.\quad x_5 = \dfrac{\mathfrak{S}p - 1 - 26 - 15}{4} = \dfrac{\mathfrak{S}p - 42}{4} = \dfrac{2.61 - 42}{4} = \dfrac{80}{4} = 20; \end{cases}$$

und 9, 34, 58 und 20 sind, wie Taf. I. zeigt, die vier ***fünften*** Stammwurzeln aus 1 zu p.

Nach (5. 10.) und nach (9.) ist

$$10.\quad p - x = 61 - 9 = 52,\ 61 - 34 = 27,\ 61 - 58 = 3 \text{ und } 61 - 20 = 41,$$

und 52, 27, 3 und 41 sind, der Tafel zufolge, die ***vier zehnten*** Stammwurzeln aus 1 zu p.

Beweis. ***A.*** Für die fünften Stammwurzeln aus 1 zu p ist

$$11.\quad x^5 = \mathfrak{G}p+1.$$

Von den *fünf* ganzzahligen Werthen >0 und $<p$, welche x für diese Gleichung nach (§. 54.) haben *kann*, und von welchen $x=1$ einer ist, sind die vier andern, >1, nothwendig die fünften *Stammwurzeln* aus 1 zu p, weil *vier* Zahlen 1, 2, 3 und 4 mit 5 keinen Theiler >1 gemein haben und also, sobald $p-1$ mit 5, oder, weil $p-1$ immer *gerade* ist, mit 10 aufgeht, und folglich p von der Form $10n+1$ ist, nach (§. 63. I.) *vier* Stammwurzeln und folglich *vier* Werthe von $x>1$ Statt finden *müssen*, die der Gleichung (11.) genugthun und die also die *vier andern* ganzzahligen Wurzeln der Gleichung (11.) sind, welche es aufser $x=1$ geben kann und für $p=10n+1$ geben *mufs*.

B. Diese vier Wurzeln der Gleichung (11.) >1 sind die der Gleichung

$$12.\quad x^4+x^3+x^2+x+1 = np;$$

denn (11.) giebt

$$13.\quad x^5-1 = (x-1)(x^4+x^3+x^2+x+1) = \mathfrak{G}p,$$

und dieser Gleichung wird durch $x=1$ und dann durch die vier andern Werthe, welche x in (12.) haben kann, entsprochen.

C. Dividirt man (12.) durch x^2, so ergiebt sich

$$14.\quad x^2+x+1+\frac{1}{x}+\frac{1}{x^2} = \frac{m}{x^2}.p.$$

Setzt man hierauf

$$15.\quad x+\frac{1}{x} = u,$$

welches $u^2=x^2+2+\frac{1}{x^2}$, also $x^2+\frac{1}{x^2}=u^2-2$ giebt, so ist (14.) soviel als

$$u^2-2+u+1 = \frac{m}{x^2}.p \text{ oder}$$

$$16.\quad u^2+u-1 = \frac{m}{x^2}.p.$$

D. Löset man diese Gleichung zweiten Grades auf die gewöhnliche Weise auf, so findet sich $u=-\frac{1}{2}\pm\sqrt{\left(\frac{1}{4}+1-\frac{m}{x^2}.p\right)}$ oder

$$17.\quad 2u = -1\pm\sqrt{\left(5-\frac{4m}{x^2}.p\right)}.$$

Ferner giebt (15.) $x^2+1=ux$ oder

$$18.\quad x^2-ux+1 = 0.$$

Löset man auch diese Gleichung zweiten Grades auf, so findet sich $x=+\frac{1}{2}u\pm\sqrt{(\frac{1}{4}u^2-1)}$ oder

$$19.\quad 4x = 2u\pm\sqrt{(4u^2-16)},$$

und hierin den Werth von $2u$ aus (17.) gesetzt,

$$4x = -1 \pm \sqrt{\left(5-\frac{4m}{x^2}.p\right)} \pm \sqrt{\left[1 \mp 2\sqrt{\left(5-\frac{4m}{x^2}.p\right)} + 5 - \frac{4m}{x^2}.p - 16\right]} \text{ oder}$$

20. $$x = -\frac{1 \pm \sqrt{\left(5-\frac{4m}{x^2}.p\right)} \pm \sqrt{\left[-\frac{4m}{x^2}.p - 10 \mp 2\left(5-\frac{4m}{x^2}.p\right)\right]}}{4}.$$

E. Nun mufs dieser Ausdruck von x nothwendig für $p = 10n+1$ *vier ganzzahlige* Werthe geben, weil dann vier ganzzahlige Stammwurzeln $x > 1$ aus 1 zu p Statt finden.

Dieses ist zunächst nicht anders möglich, als wenn das unbekannte $4m$ in (14.) mit x^2 *aufgeht;* denn wäre das nicht der Fall, so wäre in (20.) $\sqrt{\left(5-\frac{4m}{x^2}.p\right)}$ eine *Irrationalzahl,* oder doch ein *Bruch;* und Ähnliches wäre $\sqrt{\left[-\frac{4m}{x^2}.p-10 \mp 2\sqrt{\left(5-\frac{4m}{x^2}.p\right)}\right]}$. Es mufs also $-\frac{4m}{x^2}$ irgend eine *ganze* Zahl $\mathfrak{S}$ sein. Dadurch reducirt sich (20.) auf

21. $$x = \frac{-1 \pm \sqrt{(\mathfrak{S}p+5)} \pm \sqrt{[\mathfrak{S}p - 10 \mp 2\sqrt{(\mathfrak{S}p+5)}]}}{4}.$$

F. Aber auch hier kann x nicht anders eine *ganze* Zahl sein, als wenn $\mathfrak{S}p+5$ irgend ein *Quadrat* z^2, also nach (1.)

22. $$z^2 = \mathfrak{S}p+5$$

ist; denn wäre das nicht, so wäre wieder in (2.) $\sqrt{(\mathfrak{S}p+5)}$ eine *Irrationalzahl* und $\sqrt{[\mathfrak{S}p - 10 \mp 2\sqrt{(\mathfrak{S}p+5)}]}$ wäre es ebenfalls.

Dadurch reducirt sich dann (21.) auf

23. $$x = \frac{-1 \pm z \pm \sqrt{(\mathfrak{S}p - 10 \mp 2z)}}{4}.$$

G. Hier ist wiederum aus denselben Gründen nöthig, dafs auch $\mathfrak{S}p - 10 \mp 2z$, oder, da für z in (22.) sowohl $+z$ als $-z$ gesetzt werden kann, $\mathfrak{S}p + 2z - 10$ irgend ein *Quadrat* y^2, folglich nach (3.)

24. $$y^2 = \mathfrak{S}p + 2z - 10$$

sei; so dafs also nach (2.) nothwendig auch $2z - 10$ *Quadratrest* zu p ist. Durch (24.) reducirt sich (23.), weil noch z sowohl $+z$ als $-z$ und y sowohl $+y$ als $-y$ ausdrückt, auf

25. $$x = \frac{-1+z+y}{4}.$$

H. Die Gleichung (25.) giebt

26. $$4x = -1+z+y.$$

Aber wenn x der Gleichung (12.) genug thut, so thut es auch $\mathfrak{S}p + x$.

Also kann man auch statt (26.)

$$27.\quad 4(\mathfrak{G}p+x) = -1+z+y$$

setzen, oder auch, wenn man $-\mathfrak{G}$ statt $4\mathfrak{G}$ schreibt,

$$28.\quad -\mathfrak{G}p+4x = -1+z+y,$$

und dies giebt schliefslich

$$29.\quad x = \frac{\mathfrak{G}p-1+z+y}{4};$$

welches der Ausdruck (4.) der vier fünften Stammwurzeln aus 1 zu p ist.

I. In (29.) oder (4.) mufs jeder der beiden Werthe, welche z in (2.) oder (1.) haben kann, ***deshalb*** je mit den beiden zu den ***andern*** Werthen von z gehörigen zwei Werthen von y in (3.) oder (24.) verbunden werden, damit für ***jeden*** Werth von x_5 in (4.) immer ***alle*** die verschiedenen Werthe von z und y in Rechnung kommen.

K. Was in (10.) von den vier ***zehnten*** Stammwurzeln aus 1 zu p behauptet wird, ist unmittelbar (§. 66. VI.) gemäfs.

L. Bekäme x in (21.) dadurch ***allein,*** dafs $+5$ Quadratrest zu p ist, ***ganzzahlige*** Werthe, so müfsten nothwendig ***deshalb allein*** fünfte Stammwurzeln aus 1 zu p Statt finden, und da dies ***nur*** dann der Fall ist, wenn $p-1$, aufser mit 2, mit 5 aufgeht, also $p=10n+1$ ist, so wäre der Umstand, dafs $+5$ Quadratrest zu p ist, auf die Stammzahlen $p=10n+1$ ***beschränkt,*** und keine andere Stammzahl $p=10n+3$, oder $p=10n-1$, oder $p=10n-3$ könnte $+5$ zum Quadratrest haben. Aber dies ist nicht der Fall. Dafs $+5$ Quadratrest zu p ist, reicht in (21.) nicht hin, sondern es mufs aufser $+5$ auch noch $2z-10$ Quadratrest zu p sein. Deshalb ist dann der Umstand, dafs $+5$ Quadratrest zu p ist, ***nicht*** auf die Stammzahlen $p=10n+1$ ***beschränkt,*** sondern auch ***andere*** Stammzahlen können $+5$ zum Quadratrest haben; wie in (I.) bemerkt.

M. Haben aber andere Stammzahlen als $p=10n+1$ zum Quadratrest $+5$, so kann zu ihnen $2z-10$ ***nicht*** Quadratrest sein; denn wäre das, so bekäme x in (21.) ***nothwendig ganzzahlige*** Werthe, und folglich fänden nothwendig auch für ***solche*** Stammzahlen fünfte Stammwurzeln aus 1 zu p Statt; was nicht der Fall ist, da für $p=10n-1$, $10n+3$ und $10n-3$, $p-1$ ***nicht*** mit 5 aufgeht. Dies wird in (II.) bemerkt.

Zu $p=29$ z. B. ist $+5$ Quadratrest und zwar zu $z=11$ und 18. Aber in $2z-10=2.11-10=12$, $=2.18-10=26$, $=2.-11-10$ $=-32=\mathfrak{G}p+26=2.-18-10=-46=\mathfrak{G}p+12$ sind 12 und 26 ***nicht*** Quadratreste zu $p=29$.

Anm. *N*. Man könnte hier wieder, ähnlich wie im vorigen Paragraph, vermittels des Gegenseitigkeitsgesetzes für Quadratreste finden, ***welche Form*** p haben mufs, damit $+5$ oder auch -5 Quadratrest oder Nichtquadratrest zu p sei. Weiter unten kommt indessen ein *allgemeiner* Satz vor über die ***Formen***, welche eine Stammzahl p haben mufs, damit eine ***beliebige*** gegebene positive oder negative Zahl x zu ihr Quadratrest oder Nichtquadratrest sei. Die Anwendung des Gegenseitigkeitsgesetzes auf den gegenwärtigen Fall $x=\pm 5$ kann also unterbleiben. Im vorigen Paragraph gab die Anwendung desselben auf $x=\pm 3$ schon das nöthige Beispiel. In dem gegenwärtigen und dem vorigen Paragraph kam es nur mehr auf die Ausdrücke der ***fünften und dritten Stammwurzeln*** aus 1 zu p an.

§. 70.

Aufgabe.

Die Reste, welche bleiben, wenn man die 2ten, 3ten, 4ten u. s. w. Potenzen einer beliebigen Zahl z durch eine andere gegebene Zahl $a > z$ dividirt, ohne Multiplication und Division, blofs durch Addition und Subtraction zu finden.

Beispiele für die Auflösung.

I. Es sei

1. $z = 6, \quad a = 33,$

2\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32,

3\. 6 12 18 24 30 3 9 15 21 27 0 6 12 18 24 30 3 9 15 21 27 0 6 12 18 24 30 3 9 15 21 27,

4\. 6 3 18 9 21 27 30 15 24 12 6 3 18 9 21 27 30 15 24 12 6 3 18 9 21 27 30 15 24 12 6 3.

II. Es sei

5\. $z = 15; \quad a = 41,$

6\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40,

7\. 15 30 4 19 34 8 23 38 12 27 1 16 31 5 20 35 9 24 39 13 28 2 17 32 6 21 36 10 25 40 14 29 3 18 33 7 22 37 11 26,

8\. 15 20 13 31 14 5 34 18 24 32 29 25 6 8 38 37 22 2 30 40 26 21 28 10 27 36 7 23 17 9 12 16 35 33 3 4 19 39 11 1.

III. Es sei

9\. $z = 23, \quad a = 41,$

10\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40,

11\. 23 5 28 10 33 15 38 20 2 25 7 30 12 35 17 40 22 4 27 9 32 14 37 19 1 24 6 29 11 34 16 39 21 3 26 8 31 13 36 18,

12\. 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1.

Auflösung, mit Beweis. *A*. Man schreibe die natürlichen Zahlen 1, 2, 3, 4 bis zu $a-1$ in eine horizontale Zeile (2. 6. 10.). Unter 1 setze man die Zahl z $(=6, 15, 23)$, von welcher die Reste der verschiedenen Potenzen verlangt werden.

Man addire z zu sich selbst und setze die *Summe,* im Fall sie a nicht übersteigt, wie 12 und 30 in (3. und 7.), so wie sie ist, im Fall sie aber a übersteigt, wie in (11.), wo sie 46 ist; nachdem davon a *abgezogen* worden, den Rest (5 in (11.)) unter 2.

Zu dieser Summe addire man abermals z und setze die neue Summe, im Fall sie nicht a übersteigt, wie 18 und 28 in (3. und 11.), selbst, und im Fall sie a übersteigt, wie in (7.), wo sie 45 ist, nachdem davon a abgezogen worden, den Rest (4 in (7.)) unter 3.

Dasselbe Verfahren wiederhole man und setze das Resultat unter 4; und so fort, bis zu $a-1$.

Wie leicht zu sehen, enthält dann die zweite horizontale Zeile (3. 7. und 11.) die 1, 2, 3, 4, ...fachen der Zahl z; und zwar entweder diese Vielfachen selbst, oder die *Reste,* welche bleiben, wenn von den Vielfachen a so oft abgezogen wird, als es angeht.

B. Nun ist die 1te Potenz von z, z selbst. Man schreibe z ($=6, 15, 23$) in eine *dritte* horizontale Zeile (4. 8. 12.) unter die 1 der *ersten* Zeile (2. 6. 10.).

Die 2te Potenz von z ist das *zfache* von z. Man suche dieses *zfache,* welches sich nothwendig in der 2ten Zeile finden *mufs,* weil *alle* Vielfachen von z bis zu $a-1$fachen genommen worden sind und $z<a$ ist, in der ersten Zeile auf und schreibe es unter die Zahl 2 der ersten Zeile. In (I.) ist z. B. das $z=6$fache von 6 aufzusuchen, also 6 in der *ersten* Zeile. Unter dieser 6 steht 3, und dies ist der *Rest* zum 6fachen von 6, also von $6^2=z^2$. Die Zahl 3 setzt man daher unter die 2 der ersten Zeile in die dritte Zeile. In (II.) ist das 15fache von 15 aufzusuchen, also 15 in der *ersten* Zeile. Unter 15 steht 20, also ist 20 der *Rest* zum 15fachen von 15, folglich von $15^2=z^2$. Die Zahl 20 also mufs unter die 2 der ersten Zeile (6.) gesetzt werden; ähnlich in (III.).

Ferner ist die *dritte* Potenz von z das zfache von z^2; und da es blofs auf den *Rest* zu a ankommt, so ist der *Rest* für die dritte Potenz von z, den man verlangt, der Rest zum zfachen des *Restes* von z^2. Denn wenn $z^2=\mathfrak{G}a+r$ ist, so ist $z^3=\mathfrak{G}a+rz=\mathfrak{G}a+r_1$, wenn wieder $rz=\mathfrak{G}a+r_1$ ist. Man darf also nur den Rest zu z^2 (3 in (4.), 20 in (8.) und 37 in (12.)) in der ersten Zeile aufsuchen, so geben die in der zweiten Zeile darunter stehenden Zahlen (18 in (3.), 13 in (7.) und 31 in (11.)) das zfache des Restes zu z^2 und folglich den Rest zu z^3. Man schreibe daher diese Zahlen 18, 13 und 31 in die 3te Zeile (4. 8. und 12.) unter die 3 der ersten Zeile.

Nach *derselben* Regel sucht man wieder die für die Reste der 3ten Potenz von z so eben gefundenen Zahlen 18, 13 und 31 in der ersten Zeile (2. 6. und 10.) auf und schreibt die unter denselben in der *zweiten* Zeile (3. 7. und 11.) stehenden Zahlen 9, 31 und 16 in die *dritte* Zeile unter die 4. Sie sind die Reste zu der *vierten* Potenz von z.

Eben so weiter.

Die *dritte* Zeile (4. 8. 12.) enthält also nun die gesuchten Reste zu den *verschiedenen Potenzen* von z, deren *Exponenten* in der *ersten* Zeile darüber stehen. So ist z. B. zur 25ten Potenz von $z = 6$ der Rest zu $a = 33$ gemäfs (2. und 4.) $= 21$. Der Rest zur 17ten Potenz von $z = 15$ zu $a = 41$ ist gemäfs (6. und 8.) $= 22$; der Rest zur 28ten Potenz von $z = 23$ zu $a = 41$ ist gemäfs (10. und 12.) $= 10$ u. s. w.

Es finden sich demnach auf solche Weise die Reste von allen Potenzen von z zu a *blofs* durch Addition und Subtraction, *ohne* alle Multiplication und Division.

Der *Proben* für die Rechnung giebt es mehrere.

C. Für die *zweite* Zeile ist es z. B. eine Probe, dafs zu den 2, 3fachen u. s. w. einer Zahl der *ersten* Zeile auch die 2, 3fachen u. s. w. der zugehörigen Zahlen in der *zweiten* Zeile gehören. Z. B. unter 7 in (2.) steht 9, also mufs unter $2.7 = 14$, $2.9 = 18$ unter $3.7 = 21$, $3.9 = 27$ stehen.

Ferner ist es eine Probe für die *zweite* Zeile, dafs, im Fall *a nicht* eine Stammzahl ist, sobald *eine* schon da gewesene Zahl der zweiten Zeile wiederkehrt, auch *alle folgenden* wiederkehren *müssen;* wie es sich in (3.) zeigt. Dieserhalb braucht man denn auch die zweite Zeile nur so weit zu berechnen, bis ihre *erste* Zahl wiederkehrt; alsdann kehren auch nothwendig die folgenden wieder. Ist a eine *Stammzahl,* oder auch nur eine zu z *theilerfremde* Zahl, so ist es eine Probe für die Zahlen der zweiten Zeile, dafs ihre erste Zahl, und überhaupt *keine* ihrer Zahlen, wiederkehren kann, weil alle Vielfachen einer Zahl zu einer andern ihr theilerfremden Zahl immer *verschiedene* Reste lassen. In solchem Fall müssen also die Zahlen der zweiten Zeile *alle* die Zahlen 1, 2, 3, 4, ... $a - 1$ sein.

D. Für die *dritte* Zeile ist es eine Probe, dafs das *Product* zweier beliebigen ihrer Zahlen, durch a dividirt, zum Rest die Zahl geben mufs, über welcher in der *ersten* Zeile die *Summe* derjenigen Zahlen dieser Zeile steht, die sich über den beiden mit einander multiplicirten Zahlen der dritten Zeile befinden. Denn wenn z. B. $z^m = \mathfrak{G}a + r_m$ und $z^n = \mathfrak{G}a + r_n$ ist, so stehen

die Exponenten m und n in der *ersten* Zeile und die Reste r_m und r_n in der *dritten*. Die beiden Gleichungen mit einander multiplicirt, giebt aber $z^{m+n} = \mathfrak{G}a + r_m r_n$, also mufs unter der Zahl $m+n$ der ersten Zeile, oder, wenn $m+n > a-1$ und a eine *Stammzahl* ist, unter $m+n-(a-1)$, in der dritten Zeile das Product $r_m r_n$ stehen, und wenn $r_m r_n > a$ und a eine *Stammzahl* ist, $r_m r_n - \mathfrak{G}a$; denn die Zahlen der dritten Zeile sind die *Reste* zu a, und von den höheren Potenzen von z als der $a-1$ten für eine Stammzahl a ist schon die ate der 1ten gleich, weil dann nach dem Fermatschen Lehrsatz für *jedes* z, $z^{a-1} = \mathfrak{G}p + 1$ ist, so dafs also die $(m+n-(a-1))$ten Potenzen dieselben Reste haben wie die $(m-n)$ten. Z. B. unter 8 in (10.) steht in der dritten Zeile 10 und unter 17 steht 4, also mufs unter $8+17=25$ in der dritten Zeile $10.4=40$ stehen; und so ist es auch. Unter 14 in (6.) steht in der dritten Zeile 8 und unter 37 steht 19, also mufs unter $14+37 = 51 = \mathfrak{G}41 + 11$, mithin unter der 11 der ersten Zeile $8.19 = 152 = 3.41 + 29$, also 29 stehen; was auch der Fall ist.

Ferner findet für die *dritte* Zeile auch eine ähnliche Probe Statt, wie für die zweite. Nemlich wenn die *erste* Zahl der dritten Zeile *wieder*kehrt, so müssen auch alle folgenden wiederkehren; denn wenn z. B. in $z^m = \mathfrak{G}p + r$, $r = z$ ist, so ist offenbar $z^{m+1} = \mathfrak{G}p + z^2$, $z^{m+2} = \mathfrak{G}p + z^3$ u. s. w., und z^{m+1}, z^{m+2} u. s. w. lassen also *dieselben* Reste zu a wie z^2, z^3, sobald z^m zu a den Rest von z^1 giebt. So zeigt es sich in (4. und 12.).

Ist a eine *Stammzahl* und z eine der *Hauptstammwurzeln* zu a, so kann in der dritten Zeile die erste Zahl derselben gar nicht wiederkehren; denn alle Potenzen von z geben dann verschiedene Reste. Die Zahlen der dritten Zeile müssen also in diesem Fall *alle* die Zahlen 1, 2, 3, ... $a-1$ sein, wie es sich auch z. B. in (8.) zeigt. Auch mufs, wenn a eine Stammzahl ist, unter $a-1$ der ersten Zeile, dem Fermatschen Lehrsatze gemäfs, in der dritten Zeile *immer* 1 stehen.

§. 71.

Aufgabe.

Die Reste zu berechnen, welche bleiben, wenn man eine und dieselbe, z. B. die ete Potenz der Zahlen 1, 2, 3, 4, ... mit der Zahl a dividirt, und welche $< a$ sind.

Auflösung mit Beispielen und Beweis. *A.* Es sei z eine beliebige Zahl, also eine derer 1, 2, 3, 4, ..., von welcher die Reste der eten Potenz zu a gesucht werden; so erhält man zunächst den Rest r_2 der

2ten Potenz von z zu a, wenn man z mit sich selbst multiplicirt und das Product mit a dividirt. Darauf erhält man den Rest r_4 der 4ten Potenz von z zu a, wenn man r_2 mit sich selbst multiplicirt und das Product durch a dividirt; denn wenn $z^2 = \mathfrak{G}a + r_2$ ist, so ist $z^4 = (\mathfrak{G}a + r_2)^2 = \mathfrak{G}a + r_2^2 = \mathfrak{G}a + r_4$. Aus gleichem Grunde erhält man den Rest r_8 zur $2^3 = 8$ten Potenz von z zu a, wenn man r_4 mit sich selbst multiplicirt und das Product mit a dividirt. Und so weiter die Reste r_{16}, r_{32}, r_{64}, ... der 2^4ten, 2^5ten etc. Potenzen von z zu a.

B. Nun kann nach (§. 31.) *jede* Zahl blofs durch Summirung verschiedener Potenzen *der Zahl* 2 zusammengesetzt werden. Welcher also auch der Exponent e sein mag, für den man r in

$$1.\quad z^e = \mathfrak{G}a + r$$

verlangt: immer ist derselbe die *Summe* dieser oder jener Potenzen von 2. Man darf also nur die vorhin gefundenen Reste derjenigen Potenzen von z, deren Exponenten jene Potenzen von 2 sind, welche summirt e geben, mit einander multipliciren, so findet sich das gesuchte r in (1.). Wenn z. B. $e = x_1 + x_2 + x_3 \ldots$ und $z^{x_1} = \mathfrak{G}a + r_1$, $z^{x_2} = \mathfrak{G}a + r_2$, $z^{x_3} = \mathfrak{G}a + r_3$ etc. ist, so ist

$$2.\quad z^e = z^{x_1 + x_2 + x_3 \ldots} = z^{x_1} . z^{x_2} . z^{x_3} \ldots = (\mathfrak{G}a + r_1)(\mathfrak{G}a + r_2)(\mathfrak{G}a + r_3) \ldots = \mathfrak{G}a + r_1 r_2 r_3 \ldots,$$

und folglich vermöge (1.) $r = r_1 r_2 r_3 \ldots$ oder, wenn $r_1 r_2 r_3 \ldots > a$ ist,

$$3.\quad r_1 r_2 r_3 \ldots = \mathfrak{G}a + r.$$

Gesetzt e sei 53, so ist $e = 32 + 16 + 4 + 1 = 2^0 + 2^2 + 2^4 + 2^5$. Verlangte man also den Rest der 53ten Potenz der Zahl $z = 7$ zu $a = 55$, so wäre zunächst $z^2 = 7^2 = 49$, $z^4 = 49^2 = (55 - 6)^2 = \mathfrak{G}.a + 36$, $z^8 = 36^2 = \mathfrak{G}a + 31$, $z^{16} = 31^2 = \mathfrak{G}a + 26$, $z^{32} = 26^2 = \mathfrak{G}a + 16$, und da nun $e = 1 + 4 + 16 + 32$ ist, so ergiebt sich aus (3.) $\mathfrak{G}a + r = 7.36.26.16$, also $r = 2$.

C. Nach diesem Verfahren nun berechne man von den eten Potenzen der *Stammzahlen* 2, 3, 5, 7, 11, ... die Reste zu a. Aus den Resten der eten Potenzen *dieser* $z = 2, 3, 5, 7, 11, \ldots$ lassen sich die Reste *aller übrigen* z durch Multiplication mit einander finden, weil *jede* Zahl ein *Product von Stammzahlen* ist. Wären nemlich r_1, r_2, r_3, ... die für die Stammzahlen p_1, p_2, p_3, ... gefundenen Reste zu a, so dafs

$$4.\quad p_1^e = \mathfrak{G}a + r_1,\quad p_2^e = \mathfrak{G}a + r_2,\quad p_3^e = \mathfrak{G}a + r_3,\ \ldots$$

und es würde irgend eine Zahl z durch

$$5.\quad z = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot p_3^{\varepsilon_3} \ldots,$$

bezeichnet, so wäre

$$6.\quad z^e = p_1^{e\varepsilon_1} \cdot p_2^{e\varepsilon_2} \cdot p_3^{e\varepsilon_3} \ldots = (\mathfrak{G}a + r_1)^{\varepsilon_1} (\mathfrak{G}a + r_2)^{\varepsilon_2} (\mathfrak{G}a + r_3)^{\varepsilon_3} \ldots$$
$$= \mathfrak{G}a + r_1^{\varepsilon_1} r_2^{\varepsilon_2} r_3^{\varepsilon_3} \ldots$$

und folglich für (1.)

$$7.\quad r + \mathfrak{G}a = r_1^{\varepsilon_1} r_2^{\varepsilon_2} r_3^{\varepsilon_3} \ldots$$

Der Rest der $e = 53$ten Potenz von $p_1 = 7$ zu $55 = a$ war z. B. in (*B.*) $r_1 = 2$. Für den Rest der $53 = e$ten Potenz von $p_2 = 3$ zu $55 = a$ findet sich $r_2 = 48$. Aus diesen beiden Resten $r_1 = 2$ und $r_2 = 48$ finden sich also durch (7.) schon die Reste der $e = 53$ten Potenzen zu a von allen den z, welche (5.) ausdrückt. Z. B. für $\varepsilon_1 = 3$, $\varepsilon_2 = 2$ giebt (5.) $z = 7^3 . 3^2 = 3087$ und (7.) giebt $r + \mathfrak{G}a = 2^3 . 48^2 = 8.(-7)^2 = 7$; also ist 7 der Rest der $e = 53$ten Potenz von $z = 3087$ zu $a = 55$.

D. Verlangt man nun von den Zahlen $z = 1, 2, 3, 4, \ldots$ *bis zu* a die Reste der eten Potenzen zu a, so kann man statt (5.)

$$8.\quad z = p_1^{\varepsilon_1} r_2^{\varepsilon_2} r_3^{\varepsilon_3} \ldots + \mathfrak{G}a$$

setzen, wo $\mathfrak{G}$ so anzunehmen ist, dafs $z < a$ bleibt. Alsdann lassen sich schon aus den nach (*B.*) berechneten Resten $r_1, r_2, r_3, \ldots$ für wenige Stammzahlen $p_1, p_2, p_3, \ldots$, ja selbst schon aus den Resten für eine einzelne Stammzahl p, die Reste für viele z finden.

Hätte man z. B. nach (*B.*) blofs für die eine, kleinste Stammzahl $p_1 = 2$ den Rest der $e = 53$ten Potenz zu $a = 55$ berechnet, welcher $r_1 = 52 = \mathfrak{G}p - 3$ ist, so giebt derselbe nach (7.) schon allein die Reste zu $z^2 = (-3)^2 = 9$, $z^3 = (-3)^3 = -27 = +28$, $z^4 = -3.28 = -84 = +26$, $z^5 = -3.26 = -78 = +32$ u. s. w.

E. Ist a eine *Stammzahl* und man verlangt die Reste der eten Potenzen von $z = 1, 2, 3, 4, \ldots a - 1$ zu a, so braucht man nach dem obigen Verfahren nur die Reste für die *Hälfte* der z, nemlich nur für $z = 1, 2, 3, 4, \ldots \frac{1}{2}(a-1)$ und also jedenfalls auch nur für die *Stammzahlen* $< \frac{1}{2}a$ zu berechnen; denn die Reste für die folgenden z, bis zu a, sind nach (§. 55. III.) die berechneten Reste selbst, in umgekehrter Aufeinanderfolge, wenn e *gerade*, und die Ergänzungen derselben zu a, wenn e *ungerade* ist.

§. 72.

Aufgabe.

Die sämmtlichen *Stammwurzeln,* also auch die ***Hauptstammwurzeln,*** zu einer gegebenen *Stammzahl p* zu berechnen.

Auflösung mit Beweis und Beispielen. *A.* Da nach (§. 63. IV.) die Reste der verschiedenen Potenzen jeder ***Hauptstammwurzel*** unmittelbar nicht allein die übrigen Hauptstammwurzeln, sondern auch alle andern Stammwurzeln für alle die Exponenten δ geben, die in $p-1$ aufgehen, so kommt es offenbar nur darauf an, *irgend eine der **Hauptstammwurzeln*** zu finden. Kennt man eine solche, so darf man nur die Reste ihrer verschiedenen Potenzen bis zur $p-1$ten zu p berechnen; was nach (§. 70.) durch bloſse Addition und Subtraction, also *sehr leicht* geschieht, und die Aufgabe wird weiter nach den Regeln von (§. 63. IV.) ohne viele Mühe vollständig gelöset.

B. Aber die Schwierigkeit ist, *eine* der Hauptstammwurzeln zu finden. Wie dies *ohne Versuche* mit Leichtigkeit geschehen könne, ist eine noch nicht gelösete Aufgabe.

C. Ein Mittel, nicht sowohl eine, sondern sogleich alle ***Hauptstammwurzeln*** *ohne* Versuche zu finden, ist freilich folgendes; aber es erfordert, wenn p groſs ist, *viele* Rechnung.

Nach (§. 64. III.) erhält man nemlich die Hauptstammwurzeln, wenn man von den Zahlen 1, 2, 3, 4, ... $p-1$ die Reste derjenigen ihrer Potenzen *ausschlieſst,* deren Exponenten λ_1, λ_2, λ_3, ... die in $p-1$ aufgehenden *Stammzahlen* sind. Man müſste also die Reste r in

$$1. \quad z^{\lambda} = \mathfrak{G}p + r$$

für alle die $z = 1, 2, 3, 4, \ldots\ldots p-1$, und für alle λ, welche in $p-1$ aufgehende *Stammzahlen* sind, berechnen; was nach (§. 71.) geschehen könnte. Aber diese Rechnung ist sehr weitläuftig, wenn p beträchllich groſs ist. Auch hätte man dann erst die ***Hauptstammwurzeln,*** und müſste, wenn man auch noch die übrigen Stammwurzeln verlangt, dennoch nach (*A.*) noch erst weiter die Reste aller Potenzen einer von ihnen bis zur $p-1$ten berechnen; woraus dann nach (§. 63. IV.) die übrigen Stammwurzeln sich ergeben würden.

D. Daher wird man, besonders für beträchtlich groſse p, immer noch leichter zum Ziele gelangen, wenn man durch *Versuche* erst *bloſs eine* Hauptstammwurzel zu ermitteln sucht. Ist diese gefunden, so ergiebt sich nach (*A.*) unmittelbar und leicht das Übrige.

Zu diesen Versuchen kann und wird man also die *kleinsten* Zahlen 2, 3, 5, 6, 7, 8, 10, ... nehmen, nicht 4, 9, 16 etc., denn diese sind *Quadratreste,* und kein Quadratrest ist eine Hauptstammwurzel (§. 66. III. *a.*).

Dabei lassen sich dann aber noch einige der obigen Lehrsätze von den Stammwurzeln zur Verminderung der Rechnung benutzen.

E. Gesetzt das gegebene p sei

$$2.\quad p = 541,\ \text{also}\ p-1 = 540 = 2^2.3^3.5.$$

Man setze

$$3.\quad z^{x} = \mathfrak{S}p + r$$

und lasse x die verschiedenen *Theiler* von $p-1$ bezeichnen, so dafs

4. $x = 2,3,4,5,6,9,10,12,15,18,20,27,30,36,45,54,60,90,108,135,180$ und 270 ist, so mufs nach (§. 66. VII.), wenn in (3.) z eine *Hauptstammwurzel,* das heifst eine $\delta = p-1$te Stammwurzel sein soll, erstlich für $x = \frac{1}{2}(p-1)$, $r = -1$ sein, und zweitens mufs für alle x, die *nur* in $p-1$, *nicht* in $\frac{1}{2}(p-1)$ aufgehen, r weder $+1$ noch -1 sein. Es mufs also hier für $p-1 = 540$ zunächst r in (3.) für $x = 270$ gleich -1, und dann mufs für $x = 4, 12, 20, 36, 60, 108$ und 180, welches die x sind, die *nur* in $p-1$, *nicht* in $\frac{1}{2}(p-1)$ aufgehen, r in (3.) weder $+1$ noch -1 sein.

Wollte man also nun versuchen, ob $z = 2$ eine Hauptstammwurzel zu $p = 541$ sei, so kommt es auf die 4, 12, 20, 36, 60, 108, 180 und 270ten *Potenzen von* 2 und auf ihre Reste zu p an. Es ergiebt sich $2^4 = 16$, $2^8 = 256$, $2^{12} = 2^4.2^8 = 16.256 = \mathfrak{S}p + 309$, $2^{20} = 2^8.2^{12} = 256.309 = \mathfrak{S}p + 118$, $2^{36} = 2^{12.3} = 309^3 = \mathfrak{S}p + 194$, $2^{60} = 2^{20.3} = 118^3 = \mathfrak{S}p + 15$, $2^{108} = 2^{36.3} = 194^3 = \mathfrak{S}p + 48$, $2^{180} = 2^{60.3} = 15^3 = \mathfrak{S}p + 129$. Die Rechnung wird erleichtert, wenn man *Potenzen-Tafeln* hat; z. B. diejenigen von *Vega.* Keiner der Reste zu p von der 4, 12, 20, 36, 60 und 180ten Potenz von 2 ist also weder $+1$ noch -1, und wenn man nun noch $2^{270} = 2^{180}.2^{60}.2^{20}.2^8.2^2 = 129.15.118.256.4$ berechnet, so findet sich $2^{270} = \mathfrak{S}p - 1$. Also ist $z = 2$ in der That eine der *Hauptstammwurzeln* zu $p = 541$.

Man berechne nun noch die Reste zu den verschiedenen Potenzen von 2 bis zu $p-1 = 540$ nach (§. 70.), was durch blofse Addition und Subtraction leicht ist, so lassen sich weiter aus denselben nach der Regel (§. 63. IV.) die sämmtlichen Hauptstammwurzeln, so wie die übrigen Stammwurzeln, unmittelbar entnehmen.

F. Fände sich, anders wie in dem Fall (*E.*) für $p = 541$, dafs $z = 2$ *nicht* eine Hauptstammwurzel ist, so versuche man die nächste Zahl $z = 3$.

Findet sich, dafs auch 3 keine Hauptstammwurzel ist, so versuche man $z=5$ u. s. w. Aber schon, wenn die zwei Zahlen 2 und 3 versucht sind, lassen sich wieder andere Lehrsätze zur Verminderung der weitern Rechnung benutzen.

Es sei z. B.

5. $p=41$, also $p-1=40$.

Hier sind die ***Theiler*** $\varkappa$ von $p-1$ folgende:

6. $\varkappa=2, 4, 5, 8, 10$ und 20,

und von diesen geht nur allein 8 in $p-1$ und nicht in $\frac{1}{2}(p-1)$ auf, also kommt es für $z=2$, nächst $2^{\frac{1}{2}(p-1)}=2^{20}$, nur auf 2^8 an. Es ist $2^8=16^2=256=\mathfrak{G}p+10$. Dies ist zwar weder $+1$ noch -1, aber $2^{\frac{1}{2}(p-1)}=2^{20}$ ist $2^{2.8}.2^4=10^2.16=1600=\mathfrak{G}p+1$, nicht $\mathfrak{G}p-1$, wie es sein soll; also ist 2 *nicht* eine Hauptstammwurzel zu $p=41$. Man versuche also $z=3$. Dieses giebt $3^2=9$, $3^4=81=\mathfrak{G}p-1$, $3^8=\mathfrak{G}p+1$, $3^{16}=\mathfrak{G}p+1$, $3^{20}=\mathfrak{G}p-1$; also ist auch 3 keine Hauptstammwurzel zu $p=41$. Aber es ist nun nicht weiter nöthig, noch eine andere Zahl für z zu versuchen, denn aus $2^8=\mathfrak{G}p+10$, $2^{20}=\mathfrak{G}p+1$, $3^8=\mathfrak{G}p+1$ und $3^{20}=\mathfrak{G}p-1$ folgt $(2.3)^8=6^8=\mathfrak{G}p+10$ und $(2.3)^{20}=6^{20}=\mathfrak{G}p-1$: folglich ist 6 *nothwendig* eine der Hauptstammwurzeln zu $p=41$.

Man hat also nun nach (§. 70.) die Reste der Potenzen von 6 zu berechnen. Dies giebt:

7.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40,
8.	6	12	18	24	30	36	1	7	13	19	25	31	37	2	8	14	20	26	32	38	3	9	15	21	27	33	39	4	10	16	22	28	34	40	5	11	17	23	29	35,
9.	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1.

Die Zahlen in der Reihe (9.) sind die verlangten Reste.

Nun sind die zu $p-1=40$ *theilerfremde* Zahlen >1 folgende: 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37 und 39. Zu diesen Zahlen in der Reihe (7.) gehören in der Reihe (9.) die Zahlen

10. 6, 11, 29, 19, 28, 24, 26, 34, 35, 30, 12, 22, 13, 17, 15 und 7.

Diese sind also nach (§. 63. IV.) die Hauptstammwurzeln aus 1 zu $p=41$.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{20}=2$ haben, sind 2, 6, 14, 18, 22, 26, 34 und 38. Zu diesen Zahlen in der Reihe (7.) gehören in der Reihe (9.) die Zahlen

11. 36, 39, 21, 33, 5, 2, 20 und 8.

Diese sind also nach (§. 63. IV.) die 20ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{10}=4$ haben, sind 4, 12, 28 und 36. Diese aus (7.) geben in (9.)

die Zahlen

12. 25, 4, 31 und 23;

welches die 10ten Stammwurzeln aus 1 zu p sind.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{5}=8$ haben, sind 8, 16, 24 und 32. Zu ihnen in (7.) gehören in (9.) die Zahlen

13. 10, 18, 16 und 37;

und dieses sind die 5ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40, zum gröfsten Gemeintheiler $\frac{p-1}{8}=5$ haben, sind 5, 15, 25 und 35. Zu ihnen in (7.) gehören in (9.) die Zahlen

14. 27, 3, 14 und 38;

und dies sind die 8ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{4}=10$ haben, sind 10 und 30. Zu ihnen in (7.) gehören in (9.) die Zahlen

15. 32 und 9;

und dieses sind die 4ten Stammwurzeln aus 1 zu p.

Endlich ist $p-1=40$ die 2te und 1 die erste Stammwurzel aus 1 zu p. Also sind auf diese Weise *alle* Stammwurzeln aus 1 zu p vermittels der einen Hauptstammwurzel 6 gefunden worden.

G. Meistens wird schon der Versuch von wenigen kleinen Zahlen für z hinreichen, um eine der Hauptstammwurzeln zu entdecken, und die übrige Rechnung ist dann nach der obigen Art leicht; so dafs also diese Art der Auflösung der Aufgabe meistens ohne zu grofse Mühe anwendbar ist.

Nach ihr ist die Tafel II. für die Stammzahlen bis 101 berechnet worden. Zugleich giebt diese Tafel die Reste der Potenzen von 1, 2, 3, 4, ... $p-1$, deren Exponenten die in $p-1$ aufgehenden *Stammzahlen* sind, an; auch noch, bis zu $p=29$, die Reste der Potenzen von 1, 2, 3, 4, ... $p-1$ für *alle* Exponenten von 2 bis $p-1$, nebst den Werthen von z, zu welchen die Reste gehören. Da die Tafel überall die positiven *Quadratreste* angiebt, so kann man daraus nach (§. 45.) auch unmittelbar die *negativen* Quadratreste, so wie die positiven und negativen *Nichtquadratreste* entnehmen. Die weiter folgende Tafel III. giebt an, zu welchen Stammzahlen von 3 bis 101 die Zahlen 2, 3, 4, 5, ... 100 Hauptstammwurzeln sind.

§. 73.

Andere Beweise des Wilsonschen Lehrsatzes (§. 48.), nemlich:

Dafs für jede Stammzahl $p > 1$ das Product

$$1.\quad 1.2.3.4.\ldots.(p-1) = \mathfrak{G}p-1$$

ist.

Zweiter Beweis, durch Quadratreste und Nichtquadratreste.

A. Man setze

$$2.\quad (p-1)^2 = \mathfrak{G}p+r_1,\quad (p-2)^2 = \mathfrak{G}p+r_2,\quad (p-3)^2 = \mathfrak{G}p+r_3,\ \ldots\ \ldots\ \tfrac{1}{2}(p+1)^2 = \mathfrak{G}p+r_{\frac{1}{2}(p+1)}.$$

Die r in (2.) sind *alle* verschiedenen *Quadratreste* zu p (§. 45. 5. und 6.). Die Gleichungen

$$3.\quad 1^2 = \mathfrak{G}p+r_1,\quad 2^2 = \mathfrak{G}p+r_2,\quad 3^2 = \mathfrak{G}p+r_3,\ \ldots\ \ldots\ \tfrac{1}{2}(p-1)^2 = \mathfrak{G}p+r_{\frac{1}{2}(p-1)}$$

geben *dieselben* r, wenn auch in verschiedener Aufeinanderfolge (§. 45. 5.).

B. Nun ist das ***Product*** eines *Quadratrestes* und eines *Nichtquadratrestes* ein *Nichtquadratrest* (§. 52. IV.). Multiplicirt man also z. B. $1^2 = \mathfrak{G}p+r_1$ mit irgend einem *Nichtquadratrest* ϱ_m, so erhält man $\varrho_m.1^2 = \mathfrak{G}p+\varrho_1$, wo ϱ_1 irgend ein *Nichtquadratrest* ist. Multiplicirt man $2^2 = \mathfrak{G}p+r_2$ mit *demselben* Nichtquadratrest ϱ_m, so ist in $\varrho_m.2^2 = \mathfrak{G}p+\varrho_2$, ϱ_2 irgend ein *anderer* Nichtquadratrest als ϱ_1, weil r_2 ein *anderes* r als r_1 ist. U. s. w. Also wenn man *alle* die Gleichungen (3.) mit *einem und demselben* Nichtquadratrest ϱ_m multiplicirt, so erhält man durch

$$4.\quad \varrho_m.1^2 = \mathfrak{G}p+\varrho_1,\quad \varrho_m.2^2 = \mathfrak{G}p+\varrho_2,\quad \varrho_m.3^2 = \mathfrak{G}p+\varrho_3,\ \ldots\ \ldots\ \varrho_m(p-1)^2 = \mathfrak{G}p+\varrho_{\frac{1}{2}(p-1)}$$

$\frac{1}{2}(p-1)$ *verschiedene* und folglich *alle Nichtquadratreste* ϱ, indem es deren nur $\frac{1}{2}(p-1)$ giebt, nemlich so viele als *Quadratreste* r.

C. Multiplicirt man nun die sämmtlichen Gleichungen (4.) in einander, so ergiebt sich

$$5.\quad \varrho_m^{\frac{1}{2}(p-1)}(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)}.$$

Nun ist für *jeden Nichtquadratrest* ϱ, nach (§. 49. 2.),

$$6.\quad \varrho_m^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1,$$

also giebt (5.)

$$(\mathfrak{G}p-1)(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)}\quad \text{oder}$$

$$7.\quad -(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)}.$$

D. Multiplicirt man die Gleichungen (2.) in einander, so erhält man

$$8.\quad ((p-1)(p-2)(p-3)\ldots.\tfrac{1}{2}(p+1))^2 = \mathfrak{G}p+r_1r_2r_3\ldots.r_{\frac{1}{2}(p-1)};$$

und dieses mit (7.) multiplicirt, giebt, weil nun in dem Product *alle* die Zahlen 1, 2, 3, 4, ... $p-1$ vorkommen,

9. $-(1.2.3.4\ldots.(p-1))^2 = \mathfrak{G}p + r_1 r_2 r_3 \ldots . r_{\frac{1}{2}(p-1)}\, \varrho_1 \varrho_2 \varrho_3 \ldots . \varrho_{\frac{1}{2}(p-1)}$.

E. Aber in (9.) sind rechterhand r_1, r_2, r_3, ... $r_{\frac{1}{2}(p-1)}$, ϱ_1, ϱ_2, ϱ_3, ... $\varrho_{\frac{1}{2}(p-1)}$ ebenfalls alle die Zahlen 1, 2, 3, 4, ... $p-1$, denn ihre Gesammtzahl ist $p-1$, und sie sind *alle verschieden.* Also giebt (9.)

$$-(1.2.3.4\ldots.(p-1))^2 = \mathfrak{G}p + 1.2.3.4\ldots.p-1 \text{ oder}$$

10. $-(1.2.3.4\ldots.(p-1))[1.2.3.4\ldots.(p-1)+1] = \mathfrak{G}p.$

F. Es mufs also p entweder in den Factor $1.2.3.4\ldots.p-1$, oder in den Factor $1.2.3.4\ldots.(p-1)+1$ *aufgehn.* In den ersten Factor geht es *nicht* auf, weil die einzelnen Factoren 1, 2, 3, 4, ... $p-1$ alle *kleiner als* p sind: also mufs p in den zweiten Factor aufgehen, und daher mufs

11. $1.2.3.4\ldots.(p-1)+1 = \mathfrak{G}p$

sein; woraus die Gleichung (1.) des Lehrsatzes folgt.

Dritter Beweis, durch Hauptstammwurzeln. *G.* Es sei z eine *Hauptstammwurzel* aus 1 zu p und

12. $z^x = \mathfrak{G}p + r,$

so durchläuft nach (§. 50. II.), wenn man

13. $x = 1, 2, 3, 4, \ldots. p-1$

setzt, der Rest r ebenfalls *alle* die Zahlen 1, 2, 3, 4, ... $p-1$.

H. Nun ist nach (§. 67. II.) das Product aller Reste einer δten *Stammwurzel* $= \mathfrak{G}p+1$, wenn δ *ungerade*, und $= \mathfrak{G}p-1$, wenn δ *gerade* ist. Für die *Hauptstammwurzeln* ist $\delta = p-1$ *immer* gerade, also ist für die Hauptstammwurzel

14. $1.2.3.4\ldots.p-1 = \mathfrak{G}p-1;$

und dies ist der Wilsonsche Satz.

Vierter Beweis, durch zusammengehörige Zahlen und Quadratreste. *L.* Aus den Zahlen

15. $z = 1, 2, 3, 4, \ldots. p-1$

geben *je zwei* Zahlen z_1 und z_2 aus denen (15.) gemäfs (§. 47. III.)

16. $z\, z_2 = \mathfrak{G}p + \varrho,$

wo ϱ ein beliebiger *Nichtquadratrest* zu p ist. Es sind nach (§. 47. III.) $\frac{1}{2}(p-1)$ solche Producte vorhanden, und in ihnen durchlaufen die z_1 und z_2 *alle* die Zahlen (15.), ohne dafs irgend eine mehr als einmal vorkäme.

M. Daraus folgt, dafs das Product aller der $\frac{1}{2}(p-1)$ Producte (16.) das Product *aller* der Zahlen (15.) ist; und da nun *jedes* der $\frac{1}{2}(p-1)$ Pro-

ducte (16.) $= \mathfrak{S}p + \varrho$ giebt, so ist

$$17. \quad 1.2.3.4\ldots.(p-1) = \mathfrak{S}p + \varrho^{\frac{1}{2}(p-1)}.$$

N. Aber für jeden *Nichtquadratrest* ϱ ist zufolge (§. 49. I.), und zwar zufolge des *ersten* Beweises daselbst, der *nicht* auf dem Wilsonschen Satze beruht,

$$18. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1,$$

also ist nach (17.)

$$19. \quad 1.2.3.4\ldots.(p-1) = \mathfrak{S}p - 1;$$

dem Lehrsatze gemäfs.

Weiter unten werden sich noch andere, auf andern Vordersätzen beruhende Beweise des Satzes finden.

§. 74.

Lehrsatz.

Wenn die x *in der Gleichung*

$$1. \quad a_1\overset{1}{x} + a_2\overset{2}{x} + a_3\overset{3}{x} + \ldots. + a_n\overset{n}{x} = z$$

der Reihe nach $m_1, m_2, m_3, \ldots. m_n$ ***verschiedene** Werthe haben können, während die* a *immer **dieselben** Werthe behalten, so kann die Anzahl der **verschiedenen** Werthe, welche* z *bekommen kann,*

$$2. \quad = m_1 m_2 m_3 \ldots. m_n$$

*sein; **nicht gröfser**, wohl aber kleiner.*

Beweis *A.* Zu jedem der m_1 verschiedenen Werthe, welche $\overset{1}{x}$ soll haben können, gehört ein, und *nur ein* Werth von z, wenn die übrigen x, eben wie die a, *dieselben* Werthe behalten. Also bekommt z, wenn zunächst nur $\overset{1}{x}$ *allein* seinen Werth ändert, m_1 Werthe; und nicht mehrere. Und zwar sind alle diese m_1 Werthe von z *nothwendig* von einander verschieden. Denn gesetzt, zwei verschiedene Werthe $\overset{1}{x}_1$ und $\overset{1}{x}_2$ von $\overset{1}{x}$ gäben, mit *gleichen* Werthen der übrigen x, so wie der a, *gleiche* Werthe z_1 von z, so müfste

$$3. \quad \begin{cases} a_1\overset{1}{x}_1 + a_2\overset{2}{x} + a_3\overset{3}{x} + \ldots. + a_n\overset{n}{x} = z_1 \text{ und zugleich} \\ a_1\overset{1}{x}_2 + a_2\overset{2}{x} + a_3\overset{3}{x} + \ldots. + a_n\overset{n}{x} = z_1, \end{cases}$$

also, Eins von dem Andern abgezogen,

$$4. \quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) = 0$$

sein; was nicht sein kann, insofern $\overset{1}{x}_1$ und $\overset{1}{x}_2$ nicht einander *gleich* sein sollen.

B. Bezeichnet man nun die z, welche für die verschiedenen m_1 Werthe von $\overset{1}{x}$ entstehen, während die übrigen x, so wie die a, *dieselben* Werthe behalten, durch $z_1, z_2, z_3, \dots z_{m_1}$ und läfst darauf $\overset{2}{x}$ für den ersten Werth von $\overset{1}{x}$ seine m_2 verschiedenen Werthe annehmen, so bekommt das dem ersten Werth von $\overset{1}{x}$ entsprechende z_1 gemäfs (*A.*) seinerseits m_2, *nothwendig* verschiedene Werthe. Läfst man $\overset{2}{x}$ für den zweiten Werth von $\overset{1}{x}$ seine m_2 verschiedenen Werthe annehmen, so bekommt das dem zweiten Werth von $\overset{1}{x}$ entsprechende z_2 ebenfalls m_2, *nothwendig* unter sich verschiedene Werthe. So bekommen für *jeden* der m_1 verschiedenen Werthe von $\overset{1}{x}$ die demselben entsprechenden $z_1, z_2, z_3, \dots z_{m_1}$ *jedes* m_2 unter sich verschiedene Werthe; also ergeben sich überhaupt m_1 *mal* m_2 oder $m_1 m_2$ Werthe von z, die alle *gruppenweise* unter sich verschieden sind; und *nicht mehrere*, da zu *jedem* Werth von $\overset{1}{x}$ oder $\overset{2}{x}$ *nur ein* Werth von z gehört.

C. Aber diese $m_1 m_2$ Werthe von z, aus den verschiedenen Gruppen, sind schon nicht mehr nothwendig *alle* von einander verschieden. Denn gesetzt, die beiden bestimmten Werthe $\overset{1}{x}_1$ und $\overset{2}{x}_1$ von $\overset{1}{x}$ und $\overset{2}{x}$ gäben den Werth $\overset{1}{z}$ von z und die beiden andern Werthe $\overset{1}{x}_2$ und $\overset{2}{x}_2$ von $\overset{1}{x}$ und $\overset{2}{x}$ gäben den Werth $\overset{2}{z}$ von z, beides während die übrigen x, so wie die a, *denselben* Werth behalten, so dafs also

$$5.\quad a_1\overset{1}{x}_1 + a_2\overset{2}{x}_1 + a_3\overset{3}{x} + a_4\overset{4}{x} + \dots + a_n\overset{n}{x} = z_1 \text{ und}$$

$$6.\quad a_1\overset{1}{x}_2 + a_2\overset{2}{x}_2 + a_3\overset{3}{x} + a_4\overset{4}{x} + \dots + a_n\overset{n}{x} = z_2$$

wäre, woraus, wenn man Eins vom Andern abzieht,

$$7.\quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) + a_2(\overset{2}{x}_1 - \overset{2}{x}_2) = z_1 - z_2$$

folgt, so kann allerdings in (7.) z_1 *gleich* z_2 sein; denn dies giebt vermöge (7.)

$$8.\quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) + a_2(\overset{2}{x}_1 - \overset{2}{x}_2) = 0 \quad\text{oder}\quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) = a_2(\overset{2}{x}_2 - \overset{2}{x}_1);$$

und diese Gleichung *kann* Statt finden, sobald nur die Differenzen $\overset{1}{x}_1 - \overset{1}{x}_2$ der ungleichen $\overset{1}{x}$ mit a_2 und die Differenz $\overset{2}{x}_2 - \overset{2}{x}_1$ der ungleichen $\overset{2}{x}$ mit a_1 aufgeht.

Also kann, wenn in (1.) $\overset{1}{x}$ seine m_1 und $\overset{2}{x}$ seine m_2 verschiedenen Werthe annimmt, während die übrigen x, gleich den a, dieselben Werthe

behalten, z zwar nicht *nicht mehr* als $m_1 m_2$ verschiedene Werthe bekommen, wohl aber *weniger*.

D. Bezeichnet man wieder die $m_1 m_2$ verschiedenen Werthe, welche nach (*C.*) z in (1.) dadurch bekommen kann, dafs $\overset{1}{x}$ und $\overset{2}{x}$ ihre m_1 und m_2 verschiedenen Werthe annehmen, durch $z_1, z_2, z_3, \dots z_{m_1 m_2}$ und läfst $\overset{3}{x}$ seine m_3 verschiedenen Werthe für *jeden* der Werthe von $\overset{1}{x}$ und $\overset{2}{x}$ annehmen, während die noch übrigen x, gleich den a, *dieselben* Werthe behalten, so bekommen wieder die entsprechenden $z_1, z_2, z_3, \dots$ *jedes m_3 unter sich* verschiedene Werthe, und folglich *kann*, da $m_1 m_2$ solcher z vorhanden sind, z in (1.) überhaupt $m_1 m_2$ *mal* m_3 oder $m_1 m_2 m_3$ verschiedene Werthe bekommen; und *nicht mehr*, da immer zu jedem Werth eines x *nur ein* Werth von z gehört.

E. Aber nothwendig sind diese $m_1 m_2 m_3$ von z *nicht* alle verschieden. Denn gesetzt die bestimmten Werthe $\overset{1}{x}_1$, $\overset{2}{x}_1$ und $\overset{3}{x}_1$ von $\overset{1}{x}$, $\overset{2}{x}$ und $\overset{3}{x}$ gäben den Werth z_1 von z und die andern bestimmten Werthe $\overset{1}{x}_2$, $\overset{2}{x}_2$ und $\overset{3}{x}_2$ von $\overset{1}{x}$, $\overset{2}{x}$ und $\overset{3}{x}$ gäben den Werth z_2 von z, während die übrigen x, gleich den a, *dieselben* Werthe behalten, so dafs also

$$9. \quad a_1\overset{1}{x}_1 + a_2\overset{2}{x}_1 + a_3\overset{3}{x}_1 + a_4\overset{4}{x} \dots + a_n\overset{n}{x} = z_1 \quad \text{und}$$

$$10. \quad a_1\overset{1}{x}_2 + a_2\overset{2}{x}_2 + a_3\overset{3}{x}_2 + a_4\overset{4}{x} \dots + a_n\overset{n}{x} = z_2,$$

und folglich, Eins vom Andern abgezogen,

$$11. \quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) + a_2(\overset{2}{x}_1 - \overset{2}{x}_2) + a_3(\overset{3}{x}_1 - \overset{3}{x}_2) = z_1 - z_2$$

wäre, so kann allerdings in (11.) z_1 *gleich* z_2, oder

$$12. \quad a_1(\overset{1}{x}_1 - \overset{1}{x}_2) + a_2(\overset{2}{x}_1 - \overset{2}{x}_2) = a_3(\overset{3}{x}_2 - \overset{3}{x}_1)$$

sein: denn die x, obgleich unter sich verschieden, dürfen nur von der Art sein, dafs $a_1(\overset{1}{x}_1 - \overset{1}{x}_2) + a_2(\overset{2}{x}_1 - \overset{2}{x}_2)$ mit a_3 aufgeht, so kann die Gleichung schon bestehen.

Also kann wieder, wenn in (1.) $\overset{1}{x}$ seine m_1, $\overset{2}{x}$ seine m_2 und $\overset{3}{x}$ seine m_3 verschiedenen Werthe annimmt, während die übrigen x, gleich den a, dieselben Werthe behalten, z zwar *nicht mehr* als $m_1 m_2 m_3$ verschiedene Werthe bekommen, wohl aber weniger.

F. Fährt man auf diese Weise weiter fort, nemlich für jeden der durch die Veränderung der Werthe der ersten x entstehenden Werthe von z die

folgenden x der Reihe nach ihre verschiedenen Werthe annehmen zu lassen, so folgt was der Lehrsatz behauptet.

§. 75.

Lehrsatz.

Es sei von der ganzen Zahl

$$1.\quad E = e_1 e_2 e_3 \ldots . e_n$$

jeder der Theiler e *zu jedem der übrigen theilerfremd. Ferner sei*

$$2.\quad \frac{E}{e_1} = E_1,\quad \frac{E}{e_2} = E_2,\quad \frac{E}{e_3} = E_3,\quad \ldots .\quad \frac{E}{e_n} = E_n.$$

Setzt man dann in der Gleichung

$$3.\quad E_1 x_1 + E_2 x_2 + E_3 x_3 + \ldots . + E_n x_n = \mathfrak{S}E + r,$$

in welcher $E_1, E_2, E_3, \ldots . E_n$ *nach Belieben positiv oder negativ genommen werden können, der Reihe nach*

$$4.\quad \begin{cases} x_1 = 1, 2, 3, 4, \ldots . e_1, \\ x_2 = 1, 2, 3, 4, \ldots . e_2, \\ x_3 = 1, 2, 3, 4, \ldots . e_3, \\ . \quad . \quad . \quad . \quad . \quad . \quad . \\ x_n = 1, 2, 3, 4, \ldots . e_n, \end{cases}$$

und nimmt das willkürliche $\mathfrak{S}$ *in* (3.) *so, daſs* $r > 0$ *und nicht gröſser als* E *ist, so durchläuft:*

I. *In* (3.)

$$5.\quad r \textit{ alle die Zahlen } 1, 2, 3, 4, \ldots . E;$$

und keiner dieser Werthe von r *kommt mehr als einmal vor.*

II. *Dieselben Zahlen, welche in* x_1 *und* e_1, *oder in* x_2 *und* e_2, *oder in* x_3 *und* e_3 *u. s. w. bis zu* x_n *und* e_n, *zugleich aufgehen, gehen auch in das zugehörige* r *auf.*

III. *Alle* r, *welche zu Werthen von* $x_1, x_2, x_3, \ldots . x_n$ *gehören, die der Reihe nach zu* $e_1, e_2, e_3, \ldots . e_n$, *nemlich* x_1 zu e_1, x_2 *zu* e_2, x_3 *zu* e_3 *u. s. w. theilerfremd sind, und zwar dies alles zugleich, sind auch zu* E *theilerfremd; und nur diese* r *sind es.*

Beispiel. Es sei

$$6.\quad E = 84 = 3.4.7, \quad \text{also} \quad e_1 = 3,\quad e_2 = 4,\quad e_3 = 7, \quad \text{und}$$

$$7.\quad E_1 = 28,\quad E_2 = 21 \quad \text{und} \quad E_3 = 12.$$

Zu I. Für (3.) setze man

$$8.\quad 28x_1 - 21x_2 + 12x_3 = \mathfrak{S}.84 + r.$$

Macht nun hierin nach (4.) $x_1 = 1, 2, 3,$ $x_2 = 1, 2, 3, 4$ und

$x_3 = 1, 2, 3, 4, 5, 6, 7,$ und nimmt immer $\mathfrak{G}$ so, dafs $r > 0$ und $< E+1$ ist, so ergiebt sich

9. Für $x_1 = 1$ und $x_3 =$ 1 2 3 4 5 6 7:

	1	2	3	4	5	6	7	
$r =$	19	31	43	55	67	79	7	Für $x_2 = 1$,
	82	10	22	34	46	58	70	- $x_2 = 2$,
	61	73	1	13	25	37	49	- $x_2 = 3$,
	40	52	64	76	4	16	28	- $x_2 = 4$.

10. Für $x_1 = 2$ und $x_3 =$ 1 2 3 4 5 6 7:

	1	2	3	4	5	6	7	
$r =$	47	59	71	83	11	23	35	Für $x_2 = 1$,
	26	38	50	62	74	2	14	- $x_2 = 2$,
	5	17	29	41	53	65	77	- $x_2 = 3$,
	68	80	8	20	32	44	56	- $x_2 = 4$.

11. Für $x_1 = 3$ und $x_3 =$ 1 2 3 4 5 6 7:

	1	2	3	4	5	6	7	
$r =$	75	3	15	27	39	51	63	Für $x_2 = 1$,
	54	66	78	6	18	30	42	- $x_2 = 2$,
	33	45	57	69	81	9	21	- $x_2 = 3$,
	12	24	36	48	60	72	84	- $x_2 = 4$.

Die Werthe von r in (9. 10. 11.) zusammengenommen sind alle die Zahlen 1, 2, 3, 4, ... 84, und keine kommt mehr als einmal vor; gemäfs (I.).

Zu II. Die Zahl 2 geht in $x_2 = 2$ und $e_2 = 4$ auf, und alle r, die in (9. 10. 11.) zu $x_2 = 2$ gehören, gehen ebenfalls mit 2 auf; gemäfs (II.).

Zu III. $x_1 = 2$ ist zu $e_1 = 3$, $x_2 = 3$ zu $e_2 = 4$ und $x_3 = 5$ zu $e_3 = 7$ theilerfremd; das zu $x_1 = 2$, $x_2 = 3$ und $x_3 = 5$ gehörige r ist nach (10.) $= 53$, welches zu $E = 84$ theilerfremd ist; gemäfs (III.).

Beweis *A*. Da dem x_1 in (3.) gemäfs (4.) e_1, dem x_2, e_2, dem x_3, e_3 u. s. w. verschiedene Werthe gegeben werden sollen, so *kann* $E_1x_1 + E_2x_2 + E_3x_3 + \ldots + E_nx_n$ nach (§. 74.) $e_1e_2e_3 \ldots e_n = E$ verschiedene Werthe bekommen, und *nicht mehrere;* also auch r *kann* eben so viele verschiedene Werthe bekommen, die alle > 0 und nicht gröfser als E sind. Es fragt sich nun, ob von den Werthen, welche r *wirklich* bekommt, diese oder jene für *verschiedene* $x_1, x_2, x_3, \ldots$ einander *gleich* sein können. Ist dies *nicht* der Fall, so durchläuft r nothwendig *alle* die Zahlen 1, 2, 3, 4, ... E.

B. Man setze, für die beiden Werthe $\overset{1}{x}_1$ und $\overset{2}{x}_1$ von x_1, $\overset{1}{x}_2$ und $\overset{2}{x}_2$ von x_2, $\overset{1}{x}_3$ und $\overset{2}{x}_3$ von x_3 u. s. w. hätte r *denselben* Werth, so wäre in (3.)

$$12.\quad E_1\overset{1}{x}_1+E_2\overset{1}{x}_2+E_3\overset{1}{x}_3+\ldots.+E_n\overset{1}{x}_n = \mathfrak{G}E+r,$$

und *zugleich*

$$13.\quad E_1\overset{2}{x}_1+E_2\overset{2}{x}_2+E_3\overset{2}{x}_3+\ldots.+E_n\overset{2}{x}_n = \mathfrak{G}E+r.$$

Eins von dem Andern abgezogen, giebt

$$14.\quad E_1(\overset{1}{x}_1-\overset{2}{x}_1)+E_2(\overset{1}{x}_2-\overset{2}{x}_2)+E_3(\overset{1}{x}_3-\overset{2}{x}_3)+\ldots.+E_n(\overset{1}{x}_n-\overset{2}{x}_n)=\mathfrak{G}E.$$

C. In dieser Gleichung haben z. B. E_2, E_3, E_4, ... E_n, wie aus (2.) zu sehen, sämmtlich den Theiler e_1; denn sie haben der Reihe nach *nur* die Theiler e_2, e_3, e_4, ... e_n *weniger* als E, *nicht* den Theiler e_1 *weniger*. Sodann enthält auch E selbst rechts in (14.) den Theiler e_1. Also gehen *alle* Glieder in (14.) rechts und links, *bis auf das erste* links, mit e_1 auf. Deshalb mufs nach (§. 18.) auch dieses erste Glied $E_1(\overset{1}{x}_1-\overset{2}{x}_1)$ mit e_1 *aufgehen*. Aber E_1 enthält gemäfs (2.) den Factor e_1 *nicht*, und auch keinen Theiler von e_1, weil die sämmtlichen Theiler e_2, e_3, e_4, ... e_n, die E_1 hat, nach der Voraussetzung zu e_1 *theilerfremd* sind. Also mufs e_1 in $\overset{1}{x}_1-\overset{2}{x}_1$ *allein* aufgehen. Dies aber ist nicht möglich, da $\overset{1}{x}_1$ und $\overset{2}{x}_1$ nach (4.) beide >0 und nicht gröfser als e_1 sind. Also geht e_1 *nicht* in $E_1(\overset{1}{x}_1-\overset{2}{x}_1)$ auf, sondern $E_1(\overset{1}{x}_1-\overset{2}{x}_1)$, dividirt durch e_1, ist ein *Bruch*, und keine *ganze* Zahl. Und da nun ein Bruch einer ganzen Zahl nicht gleich sein kann, wie es, um die Gleichung (14.) zu erfüllen, sein müfste, so kann diese Gleichung *nicht* Statt finden. Folglich kann *kein* r für die verschiedenen x_1, x_2, x_3, ... x_n *denselben* Werth haben. Mithin sind *alle* r *verschieden*, und folglich sind sie nach (*A.*) alle die Zahlen 1, 2, 3, 4, ... E (5.); gemäfs (I.).

D. Geht die Zahl z z. B. in x_1 und e_1 *zugleich* auf, so geht sie auch in E_2, E_3, E_4, ... E_n, so wie in E auf; denn alle diese E enthalten, wie in (*C.*) erinnert, den Theiler e_1. Desgleichen geht z nach der Voraussetzung in x_1 auf. Also geht z in *alle* Glieder der Gleichung (3.), bis zu r, auf. Mithin mufs es nach (§. 18.) auch in r aufgehen. Ganz eben so verhält es sich mit Zahlen z, die in x_2 und e_2, oder in x_3 und e_3 u. s. w. zugleich aufgehen; gemäfs (II.).

E. Man setze, eine Zahl z gehe in E und r *zugleich* auf, während x_1 zu e_1, x_2 zu e_2, x_3 zu e_3 u. s. w. *theilerfremd* ist. Da z in E aufgehen soll, so mufs es irgend einen seiner *Stammfactoren*, z. B. $p>1$, mit E, und folglich auch mit einem der *Theiler* e_1, e_2, e_3, ... e_n von E gemein haben;

aber ***nur mit einem*** dieser Theiler, z. B. mit e_1; denn da jeder der Theiler e von E zu allen übrigen der Voraussetzung nach ***theilerfremd*** sein soll, so hat jedes e ***andere*** Stammfactoren (§. 27.). Es mufs also p in r und e_1 ***zugleich*** aufgehen.

F. Nun enthalten in ***allen*** Gliedern links in (3.), bis auf das ***erste*** $E_1 x_1$, die E_2, E_3, E_4, ... E_n den Theiler e_1 (*C.*): also mufs p auch in alle diese Glieder aufgehen. So ginge denn also p in ***alle*** Glieder von (3.) rechts und links bis zu dem ***ersten*** $E_1 x_1$ auf, und deshalb müfste es nach (§. 18.) auch in $E_1 x_1$ aufgehen. Aber E_1 enthält den Theiler e_1 ***nicht***, sondern nur die Theiler e_2, e_3, e_4, ... e_n: also kann p in E_1 ***nicht*** aufgehen. Mithin müfste es in x_1 aufgehen, also hätte x_1 mit e_1 den Theiler $p > 1$ gemein. Dies ist der Voraussetzung in (*E.*) entgegen, und folglich können E und r nicht mit der Zahl z ***zugleich*** aufgehen, wenn x_1 zu e_1 ***theilerfremd*** ist.

G. Aber es reicht nicht hin, dafs x_1 zu e_1 theilerfremd sei, wenn E und r es sein sollen. Denn es könnte z, statt mit e_1, mit e_2, e_3, e_4, ... einen Theiler > 1 gemein haben. Damit alles Dieses nicht sein könne, und also wirklich r zu E völlig theilerfremd sei, mufs, aus denselben Gründen wie vorhin, ***zugleich*** auch x_2 zu e_2, x_3 zu e_3 u. s. w. theilerfremd sein. Erst dann, wenn ***alles*** dieses Statt findet, ist r zu E völlig theilerfremd; gemäfs (III.).

H. Jedes r, für welches nicht x_1 zu e_1, x_2 zu e_2, x_3 zu e_3, ... x_n zu e_n zugleich theilerfremd ist, ist ***nicht*** zu E theilerfremd. Denn, wenn auch nur allein z. B. x_1 und e_1 ***nicht*** zu einander theilerfremd wären, sondern den Stammtheiler $p > 1$ gemein hätten, so würde dieser in ***alle*** Glieder rechts und links bis auf r aufgehen und müfste daher nach (§. 18.) auch in r aufgehen, so dafs also dann E und r nicht mehr theilerfremd wären, sondern den Theiler $p > 1$ gemein hätten.

Anm. *I.* Es ändert sich an den Resultaten nichts, wenn man den x statt der Werthe (4.) folgende Werthe beilegt:

$$15.\quad \begin{cases} x_1 = 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ e_1 - 1, \\ x_2 = 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ e_2 - 1, \\ x_3 = 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ e_3 - 1, \\ \ldots\ldots\ldots\ldots\ldots \\ x_n = 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ e_n - 1. \end{cases}$$

Der Werth 0 vertritt alsdann unter den Werthen von x (15.) die Stelle der

Werthe $e_1, e_2, e_3, \ldots e_n$ in (4.); denn z. B. $x_1 = e_1$ giebt in (3.) $E_1 x_1 = E_1 e_1 = E$ (2.), also in (3.)

16. $E_2 x_2 + E_3 x_3 + E_4 x_4 + \ldots + E_n x_n = \mathfrak{S}E + r$;

und eben das giebt in (3.) der Werth 0 von x.

§. 76.

Lehrsatz.

Es seien

$$1.\quad \left\{\begin{array}{l} \mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3, \ldots \mathrm{a}_{\mathrm{m}_1}, \\ \mathrm{b}_1, \mathrm{b}_2, \mathrm{b}_3, \ldots \mathrm{b}_{\mathrm{m}_2}, \\ \mathrm{c}_1, \mathrm{c}_2, \mathrm{c}_3, \ldots \mathrm{c}_{\mathrm{m}_3}, \\ \ldots\ldots \\ \mathrm{n}_1, \mathrm{n}_2, \mathrm{n}_3, \ldots \mathrm{n}_{\mathrm{m}_\mathrm{n}} \end{array}\right.$$

n ***Reihen, die erste von*** m_1, ***die zweite von*** m_2, ***die dritte von*** m_3 ***u. s. w. Gröfsen, welche alle, entweder ihren Werthen nach, oder durch sonst etwas, von einander verschieden sind.***

Stellt man diese Gröfsen in Gruppen, jede von n ***Gröfsen, zusammen, etwa nebeneinander, und ohne weitere Rücksicht in welcher Ordnung, aber auf die Weise, dafs jede Gruppe aus jeder Reihe in*** (1.) ***nur eine Gröfse enthält, so ist die Anzahl*** x_n ***der auf solche Weise möglichen verschiedenen Gruppen oder Verbindungen***

$$2.\quad \mathrm{x}_\mathrm{n} = \mathrm{m}_1 . \mathrm{m}_2 . \mathrm{m}_3 \ldots \mathrm{m}_\mathrm{n}.$$

Beispiel. Es seien die $n = 3$ Reihen

$$3.\quad \left\{\begin{array}{lll} a_1, a_2, a_3 & \text{von} & m_1 = 3 \text{ Gröfsen,} \\ b_1, b_2 & \text{von} & m_2 = 2 \quad - \quad - \\ c_1, c_2, c_3, c_4, c_5 & \text{von} & m_3 = 5 \quad - \quad - \end{array}\right.$$

gegeben, so sind die möglichen Gruppen von $n = 3$ Gröfsen folgende:

$$4.\quad \left\{\begin{array}{lllll} a_1 b_1 c_1, & a_1 b_1 c_2, & a_1 b_1 c_3, & a_1 b_1 c_4, & a_1 b_1 c_5, \\ a_1 b_2 c_1, & a_1 b_2 c_2, & a_1 b_2 c_3, & a_1 b_2 c_4, & a_1 b_2 c_5, \\ a_2 b_1 c_1, & a_2 b_1 c_2, & a_2 b_1 c_3, & a_2 b_1 c_4, & a_2 b_1 c_5, \\ a_2 b_2 c_1, & a_2 b_2 c_2, & a_2 b_2 c_3, & a_2 b_2 c_4, & a_2 b_2 c_5, \\ a_3 b_1 c_1, & a_3 b_1 c_2, & a_3 b_1 c_3, & a_3 b_1 c_4, & a_3 b_1 c_5, \\ a_3 b_2 c_1, & a_3 b_2 c_2, & a_3 b_2 c_3, & a_3 b_2 c_4, & a_3 b_2 c_5. \end{array}\right.$$

Die Anzahl dieser Gruppen ist $30 = 3.2.5 = m_1 m_2 m_3$; gemäfs (2.).

Beweis. ***A.*** Die noch unbekannte Anzahl der möglichen *verschiedenen* Gruppen von $n-1$ Gröfsen aus den $n-1$ *ersten* Reihen (1.), also aus *allen* Reihen mit Ausnahme der *letzten,* wird ähnlich von (2.), durch x_{n-1} bezeichnet.

B. *Jede* dieser x_{n-1} Gruppen, noch mit der *ersten* Gröſse n_1 der *letzten* Reihe verbunden, giebt eine Gruppe von n Gröſsen; und die daraus entstehenden x_{n-1} Gruppen von n Gröſsen sind nothwendig alle unter einander *verschieden;* denn die x_{n-1} Gruppen von $n-1$ Gröſsen, aus welchen sie entstanden, sind es nach der *Voraussetzung.*

C. Die x_{n-1} Gruppen von $n-1$ Gröſsen, mit der *zweiten* Gröſse n_2 der *letzten* Reihe verbunden, geben auf gleiche Weise x_{n-1} sämmtlich *unter sich verschiedene* Gruppen von n Gröſsen. Zugleich sind aber diese x_{n-1} Gruppen von n Gröſsen auch alle von denen in (*B.*) verschieden: denn jene enthalten alle n_1, die gegenwärtigen alle n_2.

D. Auf diese Weise geben die x_{n-1} Gruppen von $n-1$ Gröſsen, welche aus den $n-1$ ersten Reihen aufgestellt werden können, mit *jeder* der m_n Gröſsen der *letzten* Reihe verbunden, *jede* x_{n-1}, also zusammen $m_n \cdot x_{n-1}$ Gruppen von n Gröſsen, die *alle* von einander verschieden sind; denn die erste Reihe derselben enthält aus der letzten Reihe in (1.) nur n_1, die zweite nur n_2, die dritte nur n_3 u. s. w. Die so gefundenen $m_n . x_{n-1}$ Gruppen sind aber offenbar *alle möglichen* Gruppen von n Gröſsen.

E. Da nun die Anzahl dieser letzten durch x_n bezeichnet wurde, so ist

$$5. \quad x_n = m_n \cdot x_{n-1}.$$

Hieraus folgt, $n-1$ statt n gesetzt,

$$6. \quad x_{n-1} = m_{n-1} \cdot x_{n-2},$$

und Dieses in (5.) substituirt, giebt

$$7. \quad x_n = m_n \cdot m_{n-1} \cdot x_{n-2}.$$

Ferner folgt aus (6.), $n-1$ statt n gesetzt,

$$8. \quad x_{n-2} = m_{n-2} \cdot x_{n-3},$$

und Dies in (7.) substituirt, giebt

$$9. \quad x_n = m_n \cdot m_{n-1} \cdot m_{n-2} \cdot x_{n-3}.$$

Und so weiter; zuletzt

$$x_n = m_n \cdot m_{n-1} \cdot m_{n-2} \cdot m_{n-3} \dots m_1 \text{ oder}$$

$$10. \quad x_n = m_1 \cdot m_2 \cdot m_3 \cdot m_4 \dots m_n;$$

wie in (2.).

§. 77.

Lehrsatz.

Es sei von der ganzen Zahl

$$1. \quad E = e_1 e_2 e_3 \dots e_n$$

jeder der Theiler e ***zu jedem der übrigen theilerfremd.***

Es sei ferner

2. z *eine der Zahlen* $1, 2, 3, 4, \dots E$

und man setze, für ***einen und denselben*** *Werth von* z:

$$3. \quad \begin{cases} z = m_1 e_1 + r_1, & \textit{wo } r_1 \textit{ eine der Zahlen } 0, 1, 2, 3, \dots e_1 - 1, \\ z = m_2 e_2 + r_2, & \textit{wo } r_2 \; - \; - \; - \; - \; 0, 1, 2, 3, \dots e_2 - 1, \\ z = m_3 e_3 + r_3, & \textit{wo } r_3 \; - \; - \; - \; - \; 0, 1, 2, 3, \dots e_3 - 1, \\ \dots & \dots \\ z = m_n e_n + r_n, & \textit{wo } r_n \; - \; - \; - \; - \; 0, 1, 2, 3, \dots e_n - 1 \end{cases}$$

ist. Alsdann können

I. *Für zwei verschiedene Werthe von* z *niemals* ***alle*** r ***dieselben*** *Werthe haben. Zu jedem* ***andern*** *Werth von* z *gehört eine* ***andere*** *Gruppe der* n ***Reste*** r; *und umgekehrt.*

II. *Zu den* E *verschiedenen Werthen* (2.), *welche* z *soll bekommen können, gehören* ***alle verschiedene*** *Gruppen der Werthe der* n ***Reste*** r *in* (3.), *welche* ***möglich*** *sind.*

III. *Nur diejenigen* z *sind zu* E ***theilerfremd***, *für welche* ***zugleich*** r_1 *zu* e_1, r_2 *zu* e_2, r_3 zu e_3, ... r_n *zu* e_n ***theilerfremd*** *ist.*

Beispiel. Es sei

4. $E = 60, \quad e_1 = 4, \quad e_2 = 15.$

Alsdann giebt (3.)

5.

Für z =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
r_1 =	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2
r_2 =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
Für z =	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
r_1 =	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0
r_2 =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0.

Zu I. Zu keinen *zwei* Werthen von z in (5.) gehört *dasselbe* r_1 und *zugleich dasselbe* r_2; gemäfs (I.).

Zu II. Alle *möglichen* verschiedenen Gruppen aus den 4 Werthen 0, 1, 2, 3 von r_1 und 0, 1, 2, 3, ... 14 von r_2 (3.) sind folgende:

6.

0 0	0 1	0 2	0 3	0 4	0 5	0 6	0 7	0 8	0 9	0 10	0 11	0 12	0 13	0 14
1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	1 10	1 11	1 12	1 13	1 14
2 0	2 1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	2 10	2 11	2 12	2 13	2 14
3 0	3 1	3 2	3 3	3 4	3 5	3 6	3 7	3 8	3 9	3 10	3 11	3 12	3 13	3 14

Alle diese Gruppen von r kommen in (5.) vor. Sie gehören der Reihe nach zu

$$7.\quad z=\left\{\begin{array}{ccccccccccccccc}60&16&32&48&4&20&36&52&8&24&40&56&12&28&44\\45&1&17&33&49&5&21&37&53&9&25&41&57&13&29\\30&46&2&18&34&50&6&22&38&54&10&26&42&58&14\\15&31&47&3&19&35&51&7&23&39&55&11&27&43&59,\end{array}\right.$$

also zu ***allen*** den Zahlen 1, 2, 3, ... 60; gemäfs (II.).

Zu III. Z. B. $z=19$ ist zu $E=60$ theilerfremd, und das zugehörige $r_1=3$ ist es zu $e_1=4$ und $r_2=4$ zu $e_2=15$. $z=49$ ist zu $E=60$ theilerfremd, und das zugehörige $r_1=1$ ist es zu $e_1=4$ und $r_2=4$ zu $e_2=15$. Dagegen $z=35$ ist zu $E=60$ nicht theilerfremd, und nur das zugehörige $r_1=3$ ist zu $e_1=4$ theilerfremd, nicht das zugehörige $r_2=5$ zu $e_2=15$; gemäfs (III.).

Beweis. ***A.*** Könnten für zwei ***verschiedene*** Werthe z_1 und z_2 von z (3.) ***alle*** die Reste r dieselben sein, so müfste gemäfs (3.)

$$8.\quad z_1=\overset{1}{m}_1e_1+r_1=\overset{1}{m}_2e_2+r_2=\overset{1}{m}_3e_3+r_3=\ldots=\overset{1}{m}_ne_n+r_n \text{ und } \textit{zugleich}$$

$$9.\quad z_2=\overset{2}{m}_1e_1+r_1=\overset{2}{m}_2e_2+r_2=\overset{2}{m}_3e_3+r_3=\ldots=\overset{2}{m}_ne_n+r_n$$

sein. Daraus folgt, Eins von dem Andern abgezogen,

$$10.\quad z_1-z_2=(\overset{1}{m}_1-\overset{2}{m}_1)e_1=(\overset{1}{m}_2-\overset{2}{m}_2)e_2=(\overset{1}{m}_3-\overset{2}{m}_3)e_3=\ldots=(\overset{1}{m}_n-\overset{2}{m}_n)e_n,$$

also müfste zufolge (10.) z_1-z_2 durch e_1 und ***zugleich*** auch durch e_2, e_3, e_4, ... e_n, also, da die e sämmtlich zu einander theilerfremd sein sollen, gemäfs (§. 26.) auch durch das ***Product*** $e_1e_2e_3\ldots e_n$, also durch E (1.) selbst theilbar sein. Dies aber ist nicht möglich, da z_1 und z_2 beide nicht gröfser sein sollen als E (2.) und folglich z_1-z_2 nothwendig $<E$ ist. Also können nicht ***alle*** r zugleich für zwei verschiedene Werthe von z ***dieselben*** Werthe haben; gemäfs (I.).

B. Die Reste r in (3.) können der Reihe nach e_1, e_2, e_3, ... e_n verschiedene Werthe haben, nämlich r_1 die e_1 Werthe 0, 1, 2, 3, ... e_1-1, r_2 die e_2 Werthe 0, 1, 2, 3, ... e_2-1 u. s. w. Demnach sind zufolge (§. 76.) $e_1e_2e_3\ldots e_n=E$ ***verschiedene Gruppen,*** jede mit ***einem*** Werthe ***jeder*** der n Reste r_1, r_2, r_3, ... r_n ***möglich.*** Nun gehört zu ***jedem*** der E verschiedenen Werthe 1, 2, 3, ... E (2.), welche z soll haben können, nach (I.) eine ***andere*** Gruppe der n Reste r, also müssen die E möglichen Gruppen der Reste ***alle*** Statt finden, zu den verschiedenen Werthen von z gehörend; gemäfs (II.).

C. Haben z. B. r_1 und e_1 keinen Theiler >1 gemein, so müssen auch vermöge $z=m_1e_1+r_1$ (3.) z und e_1 theilerfremd sein: denn ginge z. B. $\delta>1$

in z und e_1 zugleich auf, so müfste es auch in r_1 aufgehen, und e_1 und r_1 wären also dann *nicht* theilerfremd. Eben so müssen, wenn r_2 und e_2 theilerfremd sind, auch z und e_2 es sein; wenn r_3 und e_3 theilerfremd sind, auch z und e_3 u. s. w. Also, wenn *zugleich* r_1 zu e_1, r_2 zu e_2, r_3 zu e_3, ... r_n zu e_n theilerfremd ist, so ist es auch z zu e_1, e_2, e_3, ... e_n und folglich auch zu E (1.). Hat dagegen auch nur einer der Reste, z. B. r_1, mit e_1 einen Theiler $\delta > 1$ gemein, so mufs δ vermöge der ersten Gleichung (3.) auch in z aufgehen, und es ist also alsdann z *nicht* zu e_1 und folglich auch nicht zu E (1.) theilerfremd; gemäfs (III.).

§. 78.

Lehrsatz.

Es sei von der ganzen Zahl

$$1.\quad E = e_1 e_2 e_3 \dots e_n$$

jeder der Theiler e *zu jedem der übrigen theilerfremd.*

Es seien ferner

$$2.\ \begin{cases} 1.\ \overset{1}{d}_1,\ \overset{2}{d}_1,\ \overset{3}{d}_1,\ \dots > 1 \text{ Theiler von } e_1, \text{ die zu einander theilerfremd sind;} \\ 2.\ \overset{1}{d}_2,\ \overset{2}{d}_2,\ \overset{3}{d}_2,\ \dots > 1 \text{ Theiler von } e_2, \text{ eben so;} \\ 3.\ \overset{1}{d}_3,\ \overset{2}{d}_3,\ \overset{3}{d}_3,\ \dots > 1 \text{ Theiler von } e_3, \text{ eben so;} \\ \dots\dots\dots \\ n.\ \overset{n}{d}_n,\ \overset{n}{d}_n,\ \overset{n}{d}_n,\ \dots > 1 \text{ Theiler von } e_n, \text{ eben so;} \end{cases}$$

wo also nun die d_1, *die* d_2, *die* d_3, ... *sämmtlich andere Zahlen sind, da die* e *untereinander keinen Theiler gemein haben sollen, während die sämmtlichen* d *in* E *aufgehen.*

Bezeichnet man dann aus den Zahlenreihen

$$3.\ \begin{cases} 1.\ x_1 = 1, 2, 3, 4, \dots e_1, \\ 2.\ x_2 = 1, 2, 3, 4, \dots e_2, \\ 3.\ x_3 = 1, 2, 3, 4, \dots e_3, \\ \dots\dots \\ n.\ x_n = 1, 2, 3, 4, \dots e_n \end{cases}$$

die Anzahl

$$4.\ \begin{cases} \text{Derjenigen in (3. 1.), die mit keinem der } d_1 \text{ aufgehen, durch } \psi e_1, \\ \text{Derjenigen in (3. 2.), die mit keinem der } d_2 \text{ aufgehen, durch } \psi e_2, \\ \text{Derjenigen in (3. 3.), die mit keinem der } d_3 \text{ aufgehen, durch } \psi e_3, \\ \dots\dots\dots \\ \text{Derjenigen in (3. n.), die mit keinem der } d_n \text{ aufgehen, durch } \psi e_n, \end{cases}$$

und endlich, eben so, aus der Zahlenreihe

$$5.\quad z = 1, 2, 3, 4, \ldots E$$

die ***Anzahl***

6. ***Derjenigen, die mit keinem der sämmtlichen*** d (2.) ***aufgehen, durch*** ψE:
so ist

I. ***Die*** d ***in*** (2.) ***mögen Stammzahlen, und alle Theiler von*** e_1, e_2, e_3, ... e_n ***sein, oder nicht,***

$$7.\quad \psi e_1 . \psi e_2 . \psi e_3 \ldots \psi e_n = \psi E.$$

II. ***Schreibt man, in dem Falle, wo die*** d ***in*** (2.) ***die sämmtlichen Stammtheiler*** >1 ***der*** e ***und mithin von*** E ***sind, also für den Fall, wo*** ψe_1, ψe_2, ψe_3, ... ψe_n ***und*** ψE ***die Anzahl der zu den*** e ***und zu*** E ***theilerfremden Zahlen*** $<$ e ***und*** $<$ E ***bezeichnen, zum Unterschiede*** φ ***statt*** ψ, ***so ist eben so:***

$$8.\quad \varphi e_1 . \varphi e_2 . \varphi e_3 \ldots \varphi e_n = \varphi E.$$

Beispiel zu I. Es sei

$$9.\quad e_1 = 28,\quad e_2 = 15,\quad \text{also}\quad E = 28.15 = 420.$$

Man nehme von dem Theiler von e_1 nur den einen $\overset{1}{d}_1 = 4$, und von den Theilern von e_2 nur den einen $\overset{1}{d}_2 = 5$.

Von den Zahlen 1, 2, 3, 4, ... e_1 gehen die 7 Zahlen 4, 8, 12, 16, 20, 24 und 28 mit $\overset{1}{d}_1 = 4$ auf, also bleiben $\psi e_1 = 28 - 7 = 21$ Zahlen, die *nicht* mit $\overset{1}{d}_1$ aufgehen. Von den Zahlen 1, 2, 3, 4, ... e_2 gehen die 3 Zahlen 5, 10 und 15 mit $\overset{1}{d}_2 = 5$ auf, also bleiben $\psi e_2 = 15 - 3 = 12$ Zahlen, die *nicht* mit $\overset{1}{d}_2$ aufgehen.

Es soll also nun nach dem Lehrsatze (I.)

$$10.\quad \psi e_1 . \psi e_2 = 21.12 = 252$$

die Anzahl ψE der Zahlen aus der Reihe 1, 2, 3, 4, ... 420 sein, die weder mit $\overset{1}{d}_1 = 4$, noch mit $\overset{1}{d}_2 = 5$ aufgehen.

Zunächst gehen die $\frac{420}{4} = 105$ Zahlen 4, 8, 12, 16, ... 420 mit 4 und dann die $\frac{420}{5} = 84$ Zahlen 5, 10, 15, 20, ... 420 mit 5 auf. Aber die $\frac{420}{4.5} = 21$ Zahlen 20, 40, 80, ... 420 unter den letzteren sind schon unter denen gezählt, die mit 4 aufgehen, also sind von den 420 Zahlen 1, 2, 3, 4, ... 420 nur $105 + 84 - 21 = 168$ Zahlen als diejenigen auszuschliefsen,

die mit 4 oder mit 5 aufgehen. Es ergiebt sich daher für die Anzahl der Zahlen aus denen 1, 2, 3, 4, ... 420, die weder mit 4 noch mit 5 aufgehen, nur $420-168=252=\psi E$; wie es nach (10.) und nach (I. 7.) sein soll.

Zu II. Zu $e_1=28$ *theilerfremd* sind die $\varphi e_1=12$ Zahlen 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25 und 27. Zu $e_2=15$ sind es die $\varphi e_2=8$ Zahlen 1, 2, 4, 7, 8, 11, 13 und 14. Zu $E=420$ sind es zunächst folgende 48 Zahlen: 1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 98, 97, 101, 103, 107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199, 209, und dann die 48 andern, welche sich ergeben, wenn man die hingeschriebenen 48 Zahlen von 420 abzieht (§. 65. I.). Also ist $\varphi E = 96 = 8.12 = \varphi e_1.\varphi e_2$; wie es nach (II. 8.) sein soll.

Erster Beweis. *A.* Man setze, wie in (§. 75.):

$$11.\quad \frac{E}{e_1}=E_1,\quad \frac{E}{e_2}=E_2,\quad \frac{E}{e_3}=E_3,\quad \dots\dots \quad \frac{E}{e_n}=E_n$$

und dann die Gleichung

$$12.\quad E_1x_1+E_2x_2+E_3x_3+\dots\dots+E_nx_n = \mathfrak{S}E+r,$$

wo die x aus den Zahlen (3.) genommen sind und das willkürliche $\mathfrak{S}$ so angenommen wird, dafs r nicht gröfser sei als E.

In dieser Gleichung gehört nach (§. 75.) zu jedem andern x ein anderes r, und wenn die x alle die Zahlen (3.) durchlaufen, so durchlaufen die r *alle* die Zahlen (5.).

B. Gesetzt nun ein x_1 (3. 1.) gehe *nicht* mit dem Theiler $\overset{1}{d}_1$ von e_1 (2.) auf, so kann auch das zugehörige r nicht mit $\overset{1}{d}_1$ aufgehen, und umgekehrt. Denn $E_2, E_3, E_4, \dots. E_n$ und E enthalten sämmtlich e_1 als Factor, also ist $\overset{1}{d}_1$ von den *sämmtlichen* Gliedern von (12.), bis auf das *erste* E_1x_1 und bis auf r, ein Theiler. Geht nun $\overset{1}{d}_1$ *nicht* in x_1 auf, so geht es auch nicht in E_1x_1 auf, denn E_1 (11.) enthält e_1 *nicht* als Theiler und folglich auch $\overset{1}{d}_1$ nicht, da die *Stammtheiler* von e_1, und folglich von $\overset{1}{d}_1$, in $e_2, e_3, e_4, \dots. e_n$ und mithin in $E_1=e_2e_3e_4\dots.e_n$ *nicht* vorkommen. Also kann $\overset{1}{d}_1$, da es in E_1x_1 nicht aufgeht, auch in r nicht aufgehen. Umgekehrt kann $\overset{1}{d}_1$, wenn es in r nicht aufgeht, in E_1x_1 nicht aufgehen, und folglich, da $\overset{1}{d}_1$ in E_1 nicht aufgeht, in x_1 nicht, denn sonst wäre $\frac{E_1x_1}{\overset{1}{d}_1}$ eine ganze Zahl und $\frac{r}{\overset{1}{d}_1}$ nicht.

C. Es gehört daher zu jedem x_1, welches mit $\overset{1}{d}_1$ *nicht* aufgeht, ein r, das heifst eine der Zahlen aus der Reihe der (5.), und *nur* eine, die ebenfalls mit $\overset{1}{d}_1$ *nicht* aufgeht.

Eben so gehört zu jedem x_1, welches mit $\overset{2}{d}_1$, mit $\overset{3}{d}_1$ u. s. w. nicht aufgeht, ein r, und nur eins, und immer ein anderes r zu jedem andern x_1.

Giebt es also unter den Zahlen $x_1 = 1, 2, 3, 4, \ldots e_1$ (3. 1.), ψe_1 verschiedene Zahlen, die mit *keinem* der d_1 (2. 1.) aufgehen, so giebt es *eben so viele verschiedene* dazu gehörige r, die ebenfalls mit keinem der d_1 aufgehen.

D. Auf gleiche Weise folgt, dafs, wenn es unter den Zahlen x_2, x_3, x_4, ... x_n (3.) der Reihe nach ψe_2, ψe_3, ψe_4, ... ψe_n verschiedene Zahlen giebt, die der Reihe nach mit keinem d_2, d_3, d_4, ... d_n aufgehen, *eben so viele verschiedene* r aus der Reihe der Zahlen (5.) ebenfalls mit keinem d_2, d_3, d_4, ... d_n aufgehen werden.

E. Legt man nun in der Gleichung (12.) den x der Reihe nach die ψe_1, ψe_2, ψe_3, ... ψe_n verschiedenen Werthe bei, die der Reihe nach mit den d_1, d_2, d_3, ... d_n *nicht* aufgehen, so bekommt dadurch nach (§. 74.) $\mathfrak{S}E + r$, oder, was dasselbe ist, r, $\psi e_1 . \psi e_2 . \psi e_3 \ldots . \psi e_n$ verschiedene Werthe; woraus denn folgt, dafs es gerade eben so viele verschiedene r, das heifst Zahlen aus der Reihe der (5.) giebt, die mit den verschiedenen d (2.) *nicht* aufgehen; und da nun die Anzahl dieser Zahlen in (6.) durch ψE bezeichnet wurde, so folgt dafs

$$13. \quad \psi e_1 . \psi e_2 . \psi e_3 \ldots . \psi e_n = \psi E$$

ist; gemäfs (I. 7.).

F. Die Gleichung (II. 8.) folgt unmittelbar aus (7.), denn Alles in dem Beweise bleibt *dasselbe*, wenn man für die Bedeutung des Zeichens φ statt ψ, die d in (2.) die *sämmtlichen Stammtheiler* von e_1, e_2, e_3, ... e_n, also von E bezeichnen läfst.

Zweiter Beweis. *G.* Man setze wie in (§. 77.)

$$14. \begin{cases} 1. \quad z = m_1 e_1 + r_1, \text{ wo } r_1 \text{ eine der Zahlen } 0, 1, 2, 3, \ldots e_1 - 1 \text{ ist,} \\ 2. \quad z = m_2 e_2 + r_2, \text{ wo } r_2 \text{ - - - - } 0, 1, 2, 3, \ldots e_2 - 1 \text{ ist,} \\ 3. \quad z = m_3 e_3 + r_3, \text{ wo } r_3 \text{ - - - - } 0, 1, 2, 3, \ldots e_3 - 1 \text{ ist,} \\ \ldots \\ n. \quad z = m_n e_n + r_n, \text{ wo } r_n \text{ - - - - } 0, 1, 2, 3, \ldots e_n - 1 \text{ ist.} \end{cases}$$

Geht hier z. B. der Theiler $\overset{1}{d}_1$ von e_1 in r_1 ***nicht*** auf, so kann er, da er in e_1 aufgeht, vermöge (14. 1.) auch in z ***nicht*** aufgehen; und umgekehrt.

Eben so verhält es sich mit den andern Theilern $\overset{2}{d}_1$, $\overset{3}{d}_1$, ... von e_1.

Also zu jedem r_1, welches weder mit $\overset{1}{d}_1$, noch mit $\overset{2}{d}_1$, $\overset{3}{d}_1$ etc. und überhaupt mit keinem d_1 aufgeht, gehört ein z, und immer ein anderes z, welches ebenfalls mit keinem d_1 aufgeht.

Setzt man demnach für die r_1 die Zahlen x_1 (3. 1.), so folgt, dafs zu den ψe_1 Zahlen r_1 oder x_1, die nach der Voraussetzung mit keinem d_1 aufgehen sollen, ***eben so viele verschiedene*** z gehören, die ebenfalls mit keinem d_1 aufgehen.

H. Auf gleiche Weise folgt, dafs zu den ψe_2, ψe_3, ... ψe_n Zahlen r_2, r_3, ... r_n, oder x_2, x_3, ... x_n (14. oder 3.), die der Reihe nach mit keinem d_2, d_3, ... d_n aufgehen, ***eben so viele verschiedene*** z gehören werden, die ebenfalls der Reihe nach nicht mit d_2, d_3, ... d_n aufgehen.

I. Legt man hierauf dem r in (14.) die ψe_1, ψe_2, ψe_3, ... ψe_n Werthe bei, welche der Reihe nach nicht mit den d_1, d_2, d_3, ... d_n aufgehen, und zwar so, dafs in (14.) die r niemals ***sämmtlich*** dieselben Werthe bekommen, so entstehen in den Gleichungen (14.) zusammengenommen nach (§. 76.) $\psi e_1 . \psi e_2 . \psi e_3 \ldots . \psi e_n$ ***verschiedene Gruppen*** der r, deren keine ***alle dieselben*** r hat. Zu jeder solcher Gruppe gehört nach (§. 77. I.) ein ***anderes*** z. Also giebt es auch $\psi e_1 . \psi e_2 . \psi e_3 \ldots . \psi e_n$ verschiedene z, die nicht mit d_1, d_2, d_3, ... d_n aufgehen; und da nun die Anzahl dieser z durch ψE bezeichnet worden ist, so ist wieder, wie in (7. und 13.),

$$15. \quad \psi e_1 . \psi e_2 . \psi e_3 \ldots . \psi e_n = \psi E.$$

K. Auch kann es keine andern z geben, welche mit den d ***nicht*** aufgingen, als diejenigen, für welche das Gleiche mit den r Statt findet. Denn geht z. B. r_1 in (14. 1.) mit dem Theiler $\overset{1}{d}_1$ von e_1 auf, so mufs vermöge der eben genannten Gleichung auch z mit $\overset{1}{d}_1$ aufgehen.

L. Die Gleichung (8.) findet sich wieder, wie in (***F.***), aus (7.) unmittelbar.

Anm. ***M.*** Weiter unten wird sich noch ein anderer, auf völlig verschiedene Vordersätze gegründeter Beweis des Lehrsatzes finden.

§. 79.

Lehrsatz.

Es seien x *und* y *zwei beliebige, zu einander theilerfremde, oder nicht theilerfremde ganze Zahlen. Ihr* ***Product*** xy *sei*

1. $xy = z.$

Es seien $d_1, d_2, d_3, \ldots. d_m$ *beliebige, unter einander theilerfremde Theiler von* y, *Stammtheiler oder Nicht-Stammtheiler. Jede Zahl aus der Reihe der Zahlen*

2. $1, 2, 3, 4, \ldots. y,$

welche mit ***keinem*** *der* d ***aufgeht,*** *werde durch* y_φ *bezeichnet, ihre* ***Anzahl,*** *wie in* (§. 78.), *durch* ψy *und, wenn* ***alle Theiler*** *von* y *berücksichtigt werden, durch* φy. *Eben so werde jede Zahl aus der Reihe der Zahlen*

3. $1, 2, 3, 4, \ldots. z,$

welche mit ***keinem*** *der* d ***aufgeht,*** *durch* z_φ *bezeichnet, ihre* ***Anzahl*** *durch* ψz *und für* ***alle*** d *durch* φz.

Alsdann ist

4. $\psi z = x.\psi y$ und $\varphi z = x.\varphi y.$

Beispiel. Es sei

5. $x = 15, \; y = 24,$ also $z = xy = 15.24 = 360.$

Man berücksichtige nur die *zwei* Theiler

6. $d_1 = 3$ und $d_2 = 4$

von $y = 24$, so sind die Zahlen y_φ aus der Reihe der Zahlen

7. $1, 2, 3, 4, \ldots. 24 \; (= y),$

welche weder mit $d_1 = 3$, noch mit $d_2 = 4$ *aufgehen,* folgende:

8. $y_\varphi = 1, 2, 5, 7, 10, 11, 13, 14, 17, 19, 22$ und 23.

Ihre *Anzahl* ist

9. $\psi y = 12.$

Dagegen sind die Zahlen z_φ aus der Reihe der Zahlen

10. $1, 2, 3, 4, \ldots. 360 \; (= z),$

welche weder mit $d_1 = 3$, noch mit $d_2 = 4$ aufgehen, folgende:

11. $z_\varphi =$ 1, 2, 5, 7, 10, 11, 13, 14, 17, 19, 22, 23,
25, 26, 29, 31, 34, 35, 37, 38, 41, 43, 46, 47,
49, 50, 53, 55, 58, 59, 61, 62, 65, 67, 70, 71,
73, 74, 77, 79, 82, 83, 85, 86, 89, 91, 94, 95,
97, 98, 101, 103, 106, 107, 109, 110, 113, 115, 118, 119,
121, 122, 125, 127, 130, 131, 133, 134, 137, 139, 142, 143,
. .

Ihre Anzahl $\overset{1}{\psi} z$ ist, da es 15 Zeilen, jede zu 12 Zahlen giebt,

$$12.\quad \overset{1}{\psi} z = 15.12 = 180 = 15.\overset{1}{\psi} y = x.\overset{1}{\psi} y;$$

gemäfs (4.).

Beweis *A*. Die *sämmtlichen* Zahlen 1, 2, 3, 4, ... z, deren jede beliebige durch z_1 bezeichnet werden mag, können offenbar durch

$$13.\quad z_1 = ny + r$$

ausgedrückt werden, wenn man der Reihe nach für

$$14.\quad n = 0, 1, 2, 3, \ldots. x - 1,$$

$$15.\quad r = 1, 2, 3, 4, \ldots. y$$

setzt.

B. Geht nun r in (13.) mit einem der Theiler d von y auf, so mufs nach (§. 18.), da y mit d aufgeht, auch z_1 mit d aufgehen. Also alle z_1 in (13.), welche zu Resten r (15.) gehören, die mit einem d aufgehen, sind *keine* der Zahlen z_φ die mit keinem d aufgehen.

C. Geht dagegen r in (13.) mit *keinem* der Theiler d von y auf, so kann auch z_1 mit *keinem* dieser Theiler aufgehen; denn ginge z_1 mit einem solchen Theiler auf, so müfste nach (§. 18.), weil y damit aufgeht, auch r damit aufgehen; gegen die Voraussetzung. Also *alle* z_1 in (13.), welche zu Resten r (15.) gehören, die mit keinem d aufgehen, sind durch z_φ bezeichnete Zahlen, und es giebt *keine andern* z_φ. Gäbe es noch andere, so könnten sie nur zu Resten r gehören, die mit einem d *aufgehen;* denn die z_1, zu Resten r gehörig, welche mit *keinem* d aufgehen, sind berücksichtigt; diese zu Resten r, mit einem d aufgehend, gehörige z_1 sind aber nach (*B.*) *keine* z_φ.

D. Nun ist die Anzahl der $r = z_\varphi$ in (13. und 15.), zu einem *bestimmten* Werthe von n (14.) gehörig, gleich ψy; eben so grofs also ist die Anzahl der $z_1 = z_\varphi$ für einen *bestimmten* Werth von n. Der Werth von n in (13.) aber ist ganz *gleichgültig:* also gehören zu *jedem* der x Werthe (15.) von n, ψy Zahlen $r = z_\varphi$, und folglich eben so viele $z_1 = z_\varphi$. Mithin giebt es überhaupt $x.\psi y$ Werthe von $z_1 = z_\varphi$, die mit keinem der d aufgehen, und es ist

$$16.\quad \overset{1}{\psi} z = x.\psi y, \text{ und}$$

$$17.\quad \varphi z = x.\varphi y \text{ für } \textit{alle} \text{ Theiler von } y;$$

wie es der Lehrsatz in (4.) behauptet.

§. 80.

Lehrsatz.

Es seien** x **und** y **zwei beliebige, zu einander theilerfremde ganze Zahlen. Ihr Product** xy **sei

1. $xy = z.$

Es seien** $d_1, d_2, d_3, \ldots d_n$ **beliebige, unter einander theilerfremde Theiler von** y, **Stammtheiler oder Nicht-Stammtheiler, und** x **habe keinen dieser Theiler mit** y **gemein. Jede Zahl aus der Reihe der Zahlen

2. $1, 2, 3, 4, \ldots y,$

welche mit keinem der** d **aufgeht, werde durch** y_φ **bezeichnet, ihre Anzahl wie in** (§. 78.) **durch** ψy, **und für alle Theiler von** y **durch** φy. **Ähnlich werde jede Zahl aus der Reihe der Zahlen

3. $1, 2, 3, 4, \ldots z,$

***welche mit keinem** d **und** zugleich mit x selbst **nicht aufgeht, durch** z_φ **bezeichnet, ihre Anzahl durch** $\overset{2}{\psi} z$, **und für alle** d **durch** $\overset{2}{\varphi} z$.*

Alsdann ist

4. $\overset{2}{\psi} z = (x-1)\psi y$ und $\overset{2}{\varphi} z = (x-1)\varphi y.$

Beispiel. Es sei

5. $x = 9$, $y = 40$, also $z = xy = 9.40 = 360.$

Man berücksichtige die zwei Theiler

6. $d_1 = 4$ und $d_2 = 5$

von $y = 40$, so sind die Zahlen y_φ aus der Reihe der Zahlen

7. $y = 1, 2, 3, 4, \ldots 40 \ (= y),$

welche weder mit $d_1 = 4$, noch mit $d_2 = 5$ ***aufgehen,*** folgende:

8. y_φ = 1,2,3,6,7,9,11,13,14,17,18,19,21,22,23,26,27,29,31,33,34,37,38 und 39.

Ihre ***Anzahl*** ist

9. $\psi y = 24.$

Dagegen sind die Zahlen z_φ aus der Reihe der Zahlen

10. $1, 2, 3, 4, \ldots 360 \ (= z),$

welche weder mit 4, noch mit 5 aufgehen, und ***zugleich auch nicht mit*** $x = 9$,

11. z_φ = 1, 2, 3, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 26, 29, 31, 33, 34, 37, 38, 39,
41, 42, 43, 46, 47, 49, 51, 53, 57, 58, 59, 61, 62, 66, 67, 69, 71, 73, 74, 77, 78, 79,
82, 83, 86, 87, 89, 91, 93, 94, 97, 98, 101, 102, 103, 106, 107, 109, 111, 113, 114, 118, 119,
121, 122, 123, 127, 129, 131, 133, 134, 137, 138, 139, 141, 142, 143, 146, 147, 149, 151, 154, 157, 158, 159,
161, 163, 166, 167, 169, 173, 174, 177, 178, 179, 181, 182, 183, 186, 187, 191, 193, 194, 197, 199,
201, 202, 203, 206, 209, 211, 213, 214, 217, 218, 219, 221, 222, 223, 226, 227, 229, 231, 233, 237, 238, 239,
241, 242, 246, 247, 249, 251, 253, 254, 257, 258, 259, 262, 263, 266, 267, 269, 271, 273, 274, 277, 278,
281, 282, 283, 286, 287, 289, 291, 293, 294, 298, 299, 301, 302, 303, 307, 309, 311, 313, 314, 317, 318, 319,
321, 322, 323, 326, 327, 329, 331, 334, 337, 338, 339, 341, 343, 346, 347, 349, 353, 354, 357, 358, 359,
. .

Ihre *Anzahl* $\overset{2}{\psi} z$ ist 192 und

12. $\overset{2}{\psi} z = 192$ ist $= 8.24 = (x-1)\psi y$ (5. und 9.);

wie es der Lehrsatz in (4.) behauptet.

Beweis. *A.* Die *sämmtlichen* Zahlen $1, 2, 3, 4, \ldots . z$, deren jede beliebige durch z_1 bezeichnet werden mag, können wieder offenbar durch

13. $z_1 = ny + r$

ausgedrückt werden, wenn man der Reihe nach für

14. $n = 0, 1, 2, 3, \ldots . x-1$,

15. $r = 1, 2, 3, 4, \ldots . y$

setzt.

B. Geht nun r in (13.) mit einem der Theiler d von y auf, so mufs nach (§. 18.), weil y mit d aufgeht, auch z_1 mit d aufgehen. Also alle z_1 in (13.), welche zu Resten r (15.) gehören, die mit einem d aufgehen, sind *keine* der Zahlen z_φ, welche weder mit einem d, noch mit x aufgehen sollen.

C. Geht dagegen r in (10.) mit *keinem* der Theiler d von y auf, so kann auch z_1 mit *keinem* dieser Theiler d aufgehen; denn ginge z_1 mit einem d auf, so müfste nach (§. 18.), weil d damit aufgeht, auch r damit aufgehen; gegen die Voraussetzung. Also können sich die Zahlen z_φ, welche weder mit einem d, noch mit x aufgehen sollen, nur unter denen befinden, für welche in (13.) r mit *keinem* d aufgeht. Solcher r aus den Zahlen (15. oder 2.) giebt es nach der Voraussetzung ψy für *jedes n;* denn für *jedes n* in (13.) sind die r *dieselben.* Auch giebt es *keine andern* z_1, unter welchen sich die z_φ befinden könnten, als diejenigen, für welche r mit *keinem* d aufgeht. Denn gäbe es dergleichen, so könnten sie nur zu r gehören, die mit einem d *aufgehen,* da die andern z_1 zu den r, die mit *keinem* d aufgehen, schon berücksichtigt sind. Ein z_1, zu einem mit einem d aufgehenden r müfste aber nach (*B.*) mit d aufgehen, und wäre also kein z_φ.

D. Da es demnach nur ψy verschiedene z_1 für *jedes n* giebt, unter welchen sich die z_φ befinden können, und x verschiedene Werthe von n Statt finden (14.), diese aber für z_1 in Beziehung auf r ganz gleichgültig sind, so giebt es überhaupt nur

16. $x . \psi y$

Werthe von z_1 in (13.), die mit *keinem* d aufgehen, und unter welchen sich nur die z_φ, welche mit *keinem* d und zugleich mit x nicht aufgehen sollen, befinden können.

Es fragt sich nun aber noch, wieviele es unter den $x.\psi y$ mit keinem d aufgehenden Werthen von z_1 giebt, die *mit x aufgehen.* Schliefst man diese davon aus, so werden die z_φ übrig bleiben, die weder mit einem d, noch mit x aufgehen.

E. Die mit x aufgehenden z_1 werden offenbar durch mx bezeichnet, wo

$$17. \quad m = 1, 2, 3, 4, \ldots y$$

ist, so dafs also für sie vermöge (13.)

$$18. \quad mx = ny + r$$

sein mufs, wo r mit y keinen der Theiler d gemein hat.

F. In der Gleichung (18.) mufs aber nothwendig m mit y *keinen der Theiler d gemein haben;* denn ginge ein d in m und y zugleich auf, so müfste es nach (§. 18.) auch nothwendig in r aufgehen, und y und r hätten diesen Theiler gemein; gegen die Bedingung in (*E.*).

Also kann m je nur eine der ψy Zahlen aus der Reihe der Zahlen (17. oder 2.) sein, die mit y *keinen* der Theiler d gemein haben. Mithin giebt es unter den $x.\psi y$ Werthen von z_1, die mit y keinen Theiler d gemein haben, nur ψy verschiedene Werthe, die noch mit x aufgehen, und folglich sind nur diese noch von den $x.\psi y$ Werthen der z_1 auszuschliefsen.

Geschieht solches, so bleiben

$$19. \quad x.\psi y - \psi y = (x-1)\psi y$$

Werthe von z_1 aus der Reihe der Zahlen (3.) übrig, die weder mit einem d, *noch mit x* aufgehen. Folglich ist die durch $\overset{2}{\psi} z$ bezeichnete Anzahl dieser Zahlen

$$20. \quad \overset{2}{\psi} z = (x-1)\psi y, \text{ und}$$

$$21. \quad \overset{2}{\varphi} z = (x-1)\varphi y \text{ für } \textit{alle} \text{ Theiler } d \text{ von } y;$$

wie es der Lehrsatz in (4.) behauptet.

Anm. 1. *G.* Findet die Bedingung nicht Statt, dafs x mit y keinen der Theiler d gemein haben soll, so gehen *alle* die $x.\varphi y$ verschiedenen z_1 (16.), die mit keinem d aufgehen, auch schon mit x nicht auf. Denn ginge ein solches z_1 mit x auf, so müfste es auch mit denjenigen Theilern, die x und y gemein haben, aufgehen, und hätte also *diesen* Theiler mit y gemein; was nicht der Fall ist. Hat daher x mit y Theiler d gemein, so sind von $x.\varphi y$ Werthen von z_1, die mit y kein d gemein haben, *keine x* wegen mehr auszuschliefsen, sondern die Anzahl φz der Zahlen aus der Reihe der Zahlen (3.), welche mit keinem d und auch mit x nicht aufgehen, ist $= x.\varphi y$ selbst; wie in dem Falle des Lehrsatzes (§. 79.).

Anm. 2. *H.* Die Erwägungen in (*E.* und *F.*) sind die Hauptmomente in dem Beweise des gegenwärtigen Lehrsatzes.

§. 81.

Lehrsatz.

Wenn man eine beliebige ganze Zahl Z ***nach*** (§. 21.) ***durch***

$$1.\quad Z = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_\mu^{e_\mu}$$

ausdrückt, wo die p ***die sämmtlichen*** μ ***Stammtheiler von*** Z ***und die*** e ***beliebige ganze positive Zahlen, Null eingeschlossen, ausdrücken, dann aber das Product***

$$2.\quad p_1 p_2 p_3 \ldots p_\mu = z \quad \textit{und}$$

$$3.\quad Z = nz, \quad \textit{also} \quad n = \frac{Z}{z} = p_1^{e_1-1} \cdot p_2^{e_2-1} \cdot p_3^{e_3-1} \ldots p_\mu^{e_\mu-1}$$

setzt, und die zu z ***und*** Z ***theilerfremden Zahlen*** >0 ***und*** $<z$ ***oder*** $<Z$ ***wie oben durch*** z_φ ***und*** Z_φ, ***die Anzahl dieser*** z_φ ***und*** Z_φ ***durch*** φz ***und*** φZ ***bezeichnet, so werden***

I. ***Alle zu*** Z ***theilerfremden Zahlen*** Z_φ ***durch die zu*** z ***theilerfremden Zahlen*** z_φ ***vermittels der Gleichung***

$$4.\quad Z_\varphi = \nu z + z_\varphi$$

ausgedrückt, wenn man in derselben dem z_φ ***der Reihe nach für***

$$5.\quad \nu = 0, 1, 2, 3, \ldots n-1 \ (3.)$$

alle die Werthe giebt, die es haben kann; so dafs also blofs die zu $z = p_1 p_2 p_3 \ldots p_\mu$ ***theilerfremden Zahlen*** z_φ ***nöthig sind, um alle zu*** $Z = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \ldots p_\mu^{e_\mu}$ ***theilerfremden Zahlen*** Z_φ ***zu finden.***

II. *a.* ***Die Anzahl*** φz ***der zu*** z ***theilerfremden Zahlen*** z_φ >0 und $<z$ ***ist***

$$6.\quad \varphi z = (p_1-1)(p_2-1)(p_3-1) \ldots (p_\mu-1).$$

b. ***Die Anzahl*** φZ ***der zu*** Z ***theilerfremden Zahlen*** $Z_\varphi > 0$ ***und*** $<Z$ ***ist***

$$7.\quad \varphi Z = n\varphi z = p_1^{e_1-1} \cdot p_2^{e_2-1} \cdot p_3^{e_3-1} \ldots p_\mu^{e_\mu} \cdot (p_1-1)(p_2-1)(p_3-1) \ldots (p_\mu-1).$$

III. *a.* ***Ist der kleinste Stammtheiler*** p_1 ***von*** Z (1.) $=2$, ***und sind*** $\varkappa$ ***andere Stammtheiler*** p ***von der Form*** $2^{\tau+2}.n+1$, ***wo*** n ***nicht weiter durch*** 2 ***theilbar angenommen wird, und welches dann für*** $\tau=0$ ***die Form*** $4n+1$ ***einschliefst, die übrigen*** $\mu-\varkappa-1$ ***Stammtheiler von der Form*** $4n-1$, ***so ist***

$$8.\quad \varphi Z \ \textit{durch} \ 2^{\mu+\varkappa+\tau_1+\tau_2 \ldots +e_1-2} \ \textit{theilbar.}$$

b. ***Ist der kleinste Stammtheiler*** p_1 ***von*** Z (1.) > 2, ***so ist***

9. φZ ***durch*** $2^{\mu+\varkappa+\tau_1+\tau_2 \dots}$ ***theilbar.***

IV. *a.* ***Die Summe*** $S\varphi z$ ***der sämmtlichen zu*** z ***theilerfremden Zahlen*** $z_\varphi > 0$ ***und*** $< z$ ***ist***

10. $S\varphi z = \frac{1}{2} z \varphi z = \frac{1}{2} p_1 . p_2 . p_3 \dots . p_\mu (p_1 - 1)(p_2 - 1)(p_3 - 1) \dots (p_{\mu-1} - 1)$.

b. ***Die Summe*** $S\varphi Z$ ***der sämmtlichen zu*** Z ***theilerfremden Zahlen*** $Z\varphi > 0$ ***und*** $< Z$ ***ist***

11. $S\varphi Z = \frac{1}{2} Z \varphi Z = \frac{1}{2} n Z \varphi z = \frac{1}{2} n^2 z \varphi z = \frac{1}{2} Z^2 \frac{(p_1-1)(p_2-1)(p_3-1)\dots(p_\mu-1)}{p_1 . p_2 . p_3 \dots p_\mu}$.

Beispiel zu I. Es sei

12. $\mathbf{Z} = 360 = 2^3 . 3^2 . 5$,

also

13. $\begin{cases} p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad \mu = 3, \\ e_1 = 3, \quad e_2 = 2, \quad e_3 = 1, \\ z = 2.3.5 = 30, \\ n = \frac{\mathbf{Z}}{z} = 12. \end{cases}$

Die zu $z = 30$ theilerfremden Zahlen $z_\varphi > 0$ und $< z$ sind

14. $z_\varphi = 1, 7, 11, 13, 17, 19, 23$ und 29.

Man erhält also nach (4.) die zu $\mathbf{Z} = 360$ theilerfremden Zahlen $\mathbf{Z}_\varphi > 0$ und $< \mathbf{Z}$, wenn man zu den z_φ (14.) der Reihe 1.30; 2.30; 3.30 bis 11.30 hinzuthut. Dies giebt

15. $\mathbf{Z}_\varphi =$

1	31	61	91	121	151	181	211	241	271	301	331
7	37	67	97	127	157	187	217	247	277	307	337
11	41	71	101	131	161	191	221	251	281	311	341
13	43	73	103	133	163	193	223	253	283	313	343
17	47	77	107	137	167	197	227	257	287	317	347
19	49	79	109	139	169	199	229	259	289	319	349
23	53	83	113	143	173	203	233	263	293	323	353
29	59	89	119	149	179	209	239	269	299	329	359;

und alle diese Zahlen, und nur sie, sind wirklich zu $\mathbf{Z} = 360$ theilerfremd.

Zu II. Der Ausdruck (6.) giebt hier, zufolge (13.),

16. $\varphi z = \varphi . 30 = (2-1)(3-1)(5-1) = 1.2.4 = 8$;

und dies ist ***Anzahl*** der zu $z = 30$ theilerfremden Zahlen z_φ (14.).

Der Ausdruck (7.) giebt, da $n = 12$ und $\varphi z = 8$ ist (13. und 16.),

17. $\varphi \mathbf{Z} = 12.8 = 96$;

und dies ist die ***Anzahl*** der zu $\mathbf{Z} = 360$ theilerfremden Zahlen $\mathbf{Z}\varphi$ (15.)

Zu III. In (12.) ist der ***kleinste*** Stammtheiler p_1 von $\mathbf{Z}$ gleich 2, und nur $p_3=5$ ist von der Form $4n+1$, also $\varkappa=1$. Es soll daher nach (8.) $\varphi Z=96$ (17.) durch $2^{3+3+1-2}=2^5=32$ ***theilbar*** sein; was auch der Fall ist.

Wäre $\mathbf{Z}=3^2.5.7^3.17^2$, so wäre $z=3.5.7.17$, $\varphi z=2.4.6.16$ (6.) $=768$, $n=\frac{Z}{z}=3.7^2.17=2499$ und $\varphi\mathbf{Z}=n\varphi z$ (7.) $=2499.768$. Dies soll, da hier $p_2=5=2^2+1$ und $p_4=17=2^4+1$, also $\tau_1=0$, $\tau_2=2$, $\varkappa=2$, $\mu=4$ ist, nach (9.) durch $2^{\mu+\varkappa+\tau_1+\tau_2}=2^{4+2+0+2}=2^8=256$ theilbar sein; was auch der Fall ist.

Zu IV. Nach (10.) soll für $z=30$ (13.), also für $\varphi z=8$ (16.),

$$18. \quad S\varphi z = \tfrac{1}{2}.30.8 = 120$$

sein; und dies ist auch die ***Summe*** der zu $z=30$ theilerfremden 8 Zahlen z_φ (14.).

Nach (11.) soll für $\mathbf{Z}=360$, also für $\varphi\mathbf{Z}=96$ (17.),

$$19. \quad S\varphi\mathbf{Z} = \tfrac{1}{2}.360.96 = 17280$$

sein; und dies ist auch die Summe der zu $\mathbf{Z}=360$ theilerfremden 96 Zahlen $\mathbf{Z}_\varphi$ (15.).

Beweis von I. ***A.*** In der Gleichung

$$20. \quad \mathbf{Z}_\varphi = \nu z + z_\varphi \text{ (4.)}$$

geht

$$21. \quad z = p_1.p_2.p_3 \dots p_\mu \text{ (2.)}$$

mit ***allen*** den Stammtheilern p von $\mathbf{Z}$ (1.) auf, z_φ dagegen mit ***keinem*** derselben, weil es nach der Voraussetzung zu z ***theilerfremd*** ist. Also kann auch $\mathbf{Z}_\varphi$ in (20.) mit ***keinem*** der p aufgehen, was auch ν sei. Denn ginge $\mathbf{Z}_\varphi$ mit einem der p auf, so müfste, weil z damit aufgeht, auch z_φ mit dem p aufgehen, und folglich wäre z_φ zu z ***nicht*** theilerfremd; gegen die Voraussetzung. Also ist $\mathbf{Z}_\varphi$ in (20.) für ***jedes*** z_φ und ***jedes*** ν nothwendig zu z und folglich auch zu $\mathbf{Z}$ ***theilerfremd.***

B. Denn es giebt auch ***keine anderen*** zu $\mathbf{Z}$ theilerfremden Zahlen $\mathbf{Z}_\varphi$, als die, welche (20.) ausdrückt. Denn gäbe es eine solche, so könnte sie nur zu einem z_φ gehören, welches ***nicht*** zu z theilerfremd wäre und folglich mit irgend einem p aufginge. Geht aber z_φ mit irgend einem p auf, so müfste vermöge (20.), da z mit ***jedem*** p aufgeht, auch $\mathbf{Z}_\varphi$ mit dem p aufgehen, und wäre also zu z und folglich zu $\mathbf{Z}$ ***nicht*** theilerfremd.

C. Endlich sind alle $\mathbf{Z}_\varphi$, welche (4.) oder (20.) ausdrückt, >0 und $<\mathbf{Z}$, wenn man ν nach (5.) nicht gröfser als $n-1$ setzt; denn erst nz ist $=\mathbf{Z}$ (3.), und z_φ ist $<z$, also $(n-1)z+z_\varphi$ noch $<\mathbf{Z}$.

Mithin folgt, zusammengenommen, dafs (4.) *alle* zu $\mathbf{Z}$ theilerfremden Zahlen $\mathbf{Z}_\varphi > 0$ und $< \mathbf{Z}$ ausdrückt; wie es (I.) behauptet.

Erster Beweis von II. *D.* Alle Zahlen $y > 0$ und $< p_1^{e_1}$, die *nicht* mit dem Stammtheiler p_1 aufgehen, sind zu $p_1^{e_1}$ *theilerfremd;* denn mit welchem *andern* Stammtheiler auch y aufgehen mag: $p_1^{e_1}$ geht damit nicht auf.

E. Nun gehen von den Zahlen

$$22. \quad 1,\ 2,\ 3,\ 4,\ \ldots\ldots\ p_1^{e_1}$$

$$23. \quad \textit{nur} \text{ die Zahlen } p_1,\ 2p_1,\ 3p_1,\ 4p_1,\ \ldots\ldots\ p_1^{e_1-1}.p_1 = p_1^{e_1}$$

mit p_1 auf. Alle *zwischen* denselben liegenden, die allgemein durch $\mathfrak{S}p_1 + r$ ausgedrückt werden können, gehen nicht mit p_1 auf, weil $r < p_1$ und > 0 ist.

Die *Anzahl* der Zahlen (23.) ist $= p_1^{e_1-1}$. Werden also diese von den $p_1^{e_1}$ Zahlen (22.) *ausgeschlossen,* so bleiben $p_1^{e_1} - p_1^{e_1-1} = p_1^{e_1-1}(p_1 - 1)$ Zahlen übrig, die *nicht* mit p_1 aufgehen und die also sämmtlich zu $p_1^{e_1}$ *theilerfremd* sind. Folglich ist

$$24. \quad \varphi p_1^{e_1} = p_1^{e_1-1}(p_1 - 1).$$

Ganz aus *denselben* Gründen ist

$$25. \quad \begin{cases} \varphi p_2^{e_2} = p_2^{e_2-1}(p_2 - 1), \\ \varphi p_3^{e_3} = p_3^{e_3-1}(p_3 - 1), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi p_\mu^{e_\mu} = p_\mu^{e_\mu-1}(p_\mu - 1). \end{cases}$$

F. Nun ist allgemein nach (§. 78. 8.)

$$26. \quad \varphi p_1^{e_1}.\varphi p_2^{e_2}.\varphi p_3^{e_3} \ldots . \varphi p_\mu^{e_\mu} = \varphi\left(p_1^{e_1}.p_2^{e_2}.p_3^{e_3}\ldots . p_\mu^{e_\mu}\right) = \varphi \mathbf{Z} \text{ (1.)},$$

also ist aus (24. und 25.)

$$27. \quad \varphi \mathbf{Z} = p_2^{e_1-1}.p_2^{e_2-1}.p_3^{e_3-1}\ldots . p_\mu^{e_\mu-1}(p_1-1)(p_2-1)(p_3-1)\ldots .(p_\mu-1);$$

und dieses ist der Ausdruck (7.) von $\varphi \mathbf{Z}$ im Lehrsatze.

Zweiter Beweis von II. *G.* Es sei y eine *beliebige,* p eine *Stammzahl, die* in y *nicht* aufgeht. φy und $\varphi(py)$ bezeichne die Anzahl der zu y und py *theilerfremden* Zahlen > 0 und $< y$ und py.

Alsdann ist gemäfs (§. 80.)

$$28. \quad \varphi(py) = (p-1)\varphi y;$$

was auch y sein mag, wenn es nur nicht mit p aufgeht.

H. Setzt man nun zunächst $y = p_1$, so ist offenbar $\varphi y = p_1 - 1$; denn *alle* die $p_1 - 1$ Zahlen $1, 2, 3, 4, \ldots\ldots p_1 - 1 > 0$ und $< p_1$, und *nur*

sie, sind zu der Stammzahl p_1 *theilerfremd.* Setzt man also weiter in (28.) zugleich p_2 statt p, was in $y=p_1$ nicht aufgeht, so ergiebt sich

$$29. \quad \varphi(p_1 p_2) = (p_1-1)(p_2-1).$$

Setzt man hierauf in (28.) $p_1 p_2$ statt y und p_3 statt p, was wieder in $y=p_1 p_2$ nicht aufgeht, so ergiebt sich

$$30. \quad \varphi(p_1 p_2 p_3) = (p_3-1)\,\varphi(p_1 p_2) = (p_1-1)(p_2-1)(p_3-1) \;(29.).$$

Und so weiter, wenn man der Reihe nach $p_1 p_2 p_3$ statt y, p_4 statt p, $p_1 p_2 p_3 p_4$ statt y, p_5 statt p etc. setzt. Zuletzt findet sich

$$31. \quad \varphi(p_1 p_2 p_3 \ldots . p_\mu) \text{ oder } \varphi z \;(2.) = (p_1-1)(p_2-1)(p_3-1) \ldots . p_\mu - 1;$$

und dieses ist die Gleichung (6.) des Lehrsatzes.

I. Nun drückt zufolge (I.)

$$32. \quad Z_\varphi = \nu z + z_\varphi$$

alle zu Z theilerfremden Zahlen $Z_\varphi > 0$ und $< Z$ aus, wenn man dem ν der Reihe nach die n verschiedenen Werthe 0, 1, 2, 3, ... $n-1$ (5.) und dann dem z_φ alle die φz Werthe > 0 und $< z$ giebt, die es haben kann.

Zu *jedem* Werth von ν in (32.) gehören also φz Werthe von Z_φ, und folglich giebt es überhaupt $n \varphi z$ Werthe von Z_φ, und daher ist

$$33. \quad \varphi Z = n \varphi z = \frac{Z}{z}(p_1-1)(p_2-1)(p_3-1) \ldots . (p_\mu-1) \;(3. \text{ und } 37.)$$

$$= p_1^{e_1-1} . p_2^{e_2-1} . p_3^{e_3-1} \ldots . p_\mu^{e_\mu-1} (p_1-1)(p_2-1)(p_3-1) \ldots . (p_\mu-1) \;(1. \text{ und } 2.);$$

und dieses ist der Ausdruck (7.) des Lehrsatzes.

Beweis von III. *K.* Ist der *kleinste* Stammtheiler p, von Z, $=2$, so sind alle übrigen $\mu-1$ Stammtheiler p_2, p_3, p_4, ... p_μ *ungerade;* also geht von den μ ersten Factoren von φZ in (7.), welche *Potenzen* der p sind, *allein* $p_1^{e_1-1} = 2^{e_1-1}$ mit 2 auf, und zwar mit 2^{e_1-1}. Von den übrigen Factoren (p_1-1), (p_2-1), (p_3-1), ... $p_\mu-1$ ist der erste $p_1-1=1$ und geht also *nicht* mit 2 auf. Sodann geben die $\varkappa$ verschiedenen p, welche von der Form $2^{\tau+2}.n+1$ sein sollen, $p-1=2^{\tau+2}.n$. Jeder solcher Factor geht mit $2^{\tau+2}$ auf, also, da ihrer $\varkappa$ sein sollen, so gehen sie zusammen mit $2^{2\varkappa+\tau_1+\tau_2+\ldots}$ auf. Endlich giebt jedes der $\mu-\varkappa-1$ verschiedenen p, die von der Form $4n-1$ sind, $p-1=4n-2$, und dieses geht, was auch n sein mag, *nur* mit 2 auf; denn $\frac{4n-2}{2}=2n-1$ ist *immer* ungerade. Also gehen diese $\mu-\varkappa-1$ Factoren noch mit $2^{\mu-\varkappa-1}$ auf. Mithin geht zusammengenommen φZ mit

$$34. \quad 2^{e_1-1} . 2^{2\varkappa+\tau_1+\tau_2+\ldots} . 2^{\mu-\varkappa-1} = 2^{e_1+\varkappa+\tau_1+\tau_2+\ldots+\mu-2}$$

auf; wie es (8.) in (III. *a.*) behauptet.

L. Ist schon der *kleinste* Stammtheiler p_1 von $Z > 2$, so sind alle p ohne Ausnahme ***ungerade;*** also geht dann von den μ ersten Factoren von φZ in (7.), welche ***Potenzen*** von p sind, ***keiner*** mit 2 auf. Dagegen gehen von den übrigen μ Factoren diejenigen $\varkappa$, für welche p von der Form $2^{\tau+2}.n+1$ ist, jeder mit $2^{\tau+2}$, zusammen also mit $2^{2\varkappa+\tau_1+\tau_2+\dots}$ auf. Von den $\mu-\varkappa$ Factoren, für welche p von der Form $4n-1$ ist, geht jeder ***nur*** mit 2 auf; was noch $2^{\mu-\varkappa}$ giebt. Überhaupt also ist dann φZ durch

$$35.\quad 2^{2\varkappa+\tau_1+\tau_2\dots}.2^{\mu-\varkappa} = 2^{\varkappa+\tau_1+\tau_2\dots+\mu}$$

theilbar; wie es (9.) in (III. *b.*) behauptet.

Beweis von IV. ***M.*** Die zu einer beliebigen Zahl Z theilerfremden Zahlen >0 und $<Z$ sind nach (§. 65. I.) immer ***paarweise*** vorhanden, und die Summe jedes Paares beträgt Z. Da also φZ die Anzahl der zu Z theilerfremden Zahlen ist, so ist die Zahl der vorhandenen ***Paare*** $= \frac{1}{2}\varphi Z$, und da jedes Paar Z beträgt, so ist die Summe aller,

$$36.\quad S\varphi Z = \tfrac{1}{2}Z.\varphi Z.$$

Dies ist der erste Ausdruck von $S\varphi Z$ (11.) im Lehrsatz. Setzt man darin $\varphi Z = n\varphi z$ aus (7.), so ergiebt sich der zweite Ausdruck (11.). Setzt man hierin $Z = nz$ aus (3.), so ergiebt sich der dritte, und setzt man darin $n = \frac{Z}{z}$ aus (3.), so ergiebt sich $S\varphi Z = \frac{1}{2}\frac{Z^2}{z^2}.z\varphi z = \frac{1}{2}Z^2.\frac{\varphi z}{z}$ und vermöge (2. und 6.) der vierte Ausdruck von $S\varphi Z$ (11.).

Für $Z = z$ ist, wie in (35.),

$$37.\quad S\varphi z = \tfrac{1}{2}z.\varphi z.$$

Dieses ist der erste Ausdruck von $S\varphi z$ in (10.). Setzt man darin die Werthe von z und φz aus (2. und 6.), so ergiebt sich der zweite.

Anm. ***N.*** Der *erste* Beweis von (II.), dem ***Haupttheile*** des gegenwärtigen Lehrsatzes, bedarf zwar (I.) nicht, aber des Lehrsatzes (§. 78.) mit seinen Vorbereitungen (§. 74. 75. 76. und 77.). Der ***zweite*** Beweis von (II.) dagegen bedarf aller dieser Vordersätze ***nicht,*** sondern nur des einfachen Satzes (§. 80.). Er ist daher bei weitem kürzer als der erste, und vielleicht der kürzeste von allen, die sich von (II.) geben lassen. Er würde deshalb insbesondere für die Elemente geeignet sein.

O. Von dem Satze (§. 78.) würde sich sogar der Ausdruck (8.) für den dortigen besondern Fall (II.) umgekehrt aus dem gegenwärtigen Satze (II. 7.) ableiten lassen. Denn zerlegt man z. B. Z (1.) in zwei beliebige zu einander ***theilerfremde*** Factoren, die also jeder nur ***verschiedene*** p enthalten dürfen,

z. B. in

$$38.\quad Z = z_1 z_2 = p_1^{e_1}.p_2^{e_2}.p_3^{e_3}\ldots.p_\varkappa^{e_\varkappa} \times p_{\varkappa+1}^{e_{\varkappa+1}}.p_{\varkappa+2}^{e_{\varkappa+2}}\ldots.p_\mu^{e_\mu},$$

so ist nach (7.)

$$39.\quad \varphi z_1 = p_1^{e_1-1}.p_2^{e_2-1}.p_3^{e_3-1}\ldots.p_\varkappa^{e_\varkappa-1}(p_1-1)(p_2-1)(p_3-1)\ldots.(p_\varkappa-1),$$

$$40.\quad \varphi z_2 = p_{\varkappa+1}^{e_{\varkappa+1}-1}.p_{\varkappa+2}^{e_{\varkappa+2}-1}\ldots.p_\mu^{e_\mu-1}(p_{\varkappa+1}-1)(p_{\varkappa+2}-1)\ldots\ldots.(p_\mu-1),$$

und φz_1 (39.) mit φz_2 (40.) multiplicirt giebt nichts anderes als φZ (7.), so dafs also

$$41.\quad \varphi Z = \varphi z_1 . \varphi z_2$$

ist. Auf dieselbe Weise kann man die Factoren z_1 und z_2 weiter zerlegen, und es findet sich der Ausdruck (8.) in (§. 78.).

Weiter unten werden sich noch andere Beweise von (II.) finden, die auf völlig verschiedenen Vordersätzen beruhen.

§. 82.

Lehrsatz.

Das Product P_μ *von* ν Factoren

$$1.\quad P_\mu = \begin{cases} (a_0 + a_1 + a_2 + a_3 + \ldots. + a_\alpha) \\ \times(b_0 + b_1 + b_2 + b_3 + \ldots. + b_\beta) \\ \times(c_0 + c_1 + c_2 + c_3 + \ldots. + c_\gamma) \\ \ldots\ldots\ldots\ldots\ldots \\ \times(m_0 + m_1 + m_2 + m_3 + \ldots. + m_\mu) \\ \times(n_0 + n_1 + n_2 + n_3 + \ldots. + n_\nu) \end{cases}$$

ist

I. *die Summe von Gliedern, deren jedes* ν *Factoren, und zwar aus jeder der Reihen* (1.) *nur einen Factor enthält, also nur ein* a, *nur ein* b *u. s. w. und die sämmtlich durch*

$$2.\quad a_{\alpha_1}.b_{\beta_1}.c_{\gamma_1}\ldots.m_{\mu_1}.n_{\nu_1}$$

ausgedrückt werden, wenn man in (2.) *der Reihe nach*

$$3.\quad \begin{cases} \alpha_1 = 0,\ 1,\ 2,\ 3,\ \ldots.\ \alpha, \\ \beta_1 = 0,\ 1,\ 2,\ 3,\ \ldots.\ \beta, \\ \gamma_1 = 0,\ 1,\ 2,\ 3,\ \ldots.\ \gamma, \\ \ldots\ldots\ldots \\ \mu_1 = 0,\ 1,\ 2,\ 3,\ \ldots.\ \mu, \\ \nu_1 = 0,\ 1,\ 2,\ 3,\ \ldots.\ \nu \end{cases}$$

setzt. Keines der Glieder, welche (3. *und* 2.) *geben, fehlt, und keines kommt mehr als einmal vor.*

II. ***Die Anzahl der Glieder des Products*** P_μ (1.) ***ist***

$$4.\quad = (\alpha+1)(\beta+1)(\gamma+1)\dots(\mu+1)(\nu+1).$$

Beispiel. Es sei

$$5.\quad P_\mu = (a_0+a_1+a_2)(b_0+b_1)(c_0+c_1+c_2+c_3),$$

also

$$6.\quad \mu=3,\quad \alpha=2,\quad \beta=1,\quad \gamma=3,$$

so findet sich, wenn man wirklich multiplicirt,

$$P_\mu = (a_0b_0+a_1b_0+a_2b_0+a_0b_1+a_1b_1+a_2b_1)(c_0+c_1+c_2+c_3) \text{ oder}$$

$$7.\quad P_\mu = a_0b_0c_0+a_1b_0c_0+a_2b_0c_0+a_0b_1c_0+a_1b_1c_0+a_2b_1c_0$$
$$+a_0b_0c_1+a_1b_0c_1+a_2b_0c_1+a_0b_1c_1+a_1b_1c_1+a_2b_1c_1$$
$$+a_0b_0c_2+a_1b_0c_2+a_2b_0c_2+a_0b_1c_2+a_1b_1c_2+a_2b_1c_2$$
$$+a_0b_0c_3+a_1b_0c_3+a_2b_0c_3+a_0b_1c_3+a_1b_1c_3+a_2b\,c_3.$$

Alle diese Glieder giebt (2.), wenn man darin der Reihe nach zufolge (3.) $\alpha_1=0,1,2$, $\beta_1=0,1$ und $\gamma_1=0,1,2,3$ setzt. Die Anzahl der Glieder in (7.) ist $24=3.2.4=(\alpha+1)(\beta+1)(\gamma+1)$; gemäfs (4.).

Beweis ***A.*** Man setze einen Augenblick *voraus*, das Product $P_{\nu-1}$ der ersten $\nu-1$ Reihen rechts in (1.) mit den $a, b, c, \dots m$, also das Product *aller* Reihen (1.) *bis auf die letzte* $n_0+n_1+n_2+\dots+n_\nu$, erfülle was der Lehrsatz in (I.) behauptet, nemlich, dafs das Product $P_{\nu-1}$ die Gesammtheit *aller* der Producte sei, welche nach (2.) hier durch

$$8.\quad a_{\alpha_1}.b_{\beta_1}.c_{\gamma_1}\dots l_{\lambda_1}.m_{\mu_1}$$

ausgedrückt werden, wenn man in (8.) den $\alpha_1, \beta_1, \gamma_1, \dots \mu_1$ die Werthe (3.) giebt; desgleichen setze man voraus, dafs kein a, b, c etc. in einem der Producte (8.) mehr als einmal vorkomme, und kein Product von denen, welche (8.) giebt, fehle und keines mehr als einmal sich zeige.

B. Multiplicirt man alsdann diese Gesammtheit der Producte (8.) noch mit der letzten Reihe $n_0+n_1+n_2+\dots+n_\nu$, um P_ν (1.) zu finden, so sind alle die Glieder (8.) erst mit n_0, dann mit n_1, darauf mit n_2 u. s. w. bis zu n_ν zu multipliciren. Also wird auch die Gesammtheit des neuen Products P_ν durch

$$9.\quad a_{\alpha_1}.b_{\beta_1}.c_{\gamma_1}\dots l_{\lambda_1}.m_{\mu_1}.n_{\nu_1}$$

ausgedrückt, und zwar so, dafs allen Gliedern, die (8.) giebt, noch der Factor n mit allen den Zeigern $0, 1, 2, 3, \dots \nu$, welche ν_1 bezeichnet, hinzugefügt ist. Hier fehlt kein Product in Beziehung auf n, und keines kommt mehr als einmal vor.

Also, *wenn* der Satz für $\nu-1$ Reihen in (11.) gilt, so gilt er auch für ν Reihen.

B. Daraus folgt, dafs der Satz für $\nu-1$ Reihen gilt, und folglich nach (*A.*) für ν Reihen, wenn er für $\nu-2$ Reihen gilt; ferner für $\nu-2$ Reihen, und folglich nach (*A.*) für $\nu-1$ und ν Reihen, wenn er für $\nu-3$ Reihen gilt; u. s. w. Zuletzt also folgt, dafs der Satz für ν Reihen gilt, wenn er für $\nu-(\nu-1)=1$ Reihe gilt.

Für 1 Reihe $a_0+a_1+a_2+\ldots\ldots+a_\alpha$ aber gilt er offenbar: denn alle Glieder dieser Reihe drückt a_{α_1} (8) aus, wenn man nach (3.) der Reihe nach $\alpha_1=0, 1, 2, 3, \ldots\ldots \alpha$ setzt: also gilt (I.) für beliebige ν Reihen in P_ν wirklich.

C. Man setze, die noch unbekannte *Anzahl* der Glieder des Products $P_{\nu-1}$ der ersten $\nu-1$ Reihen in (1.) sei $=x_\mu$.

Wird dieses Product $P_{\nu-1}$ noch mit der letzten Reihe $n_0+n_1+n_2+\ldots\ldots+n_\nu$ multiplicirt, um P_ν zu finden, so ergeben sich zuerst x_μ sämmtlich verschiedene Glieder, die sämmtlich n_0 zum Factor haben; sodann x_μ andere Glieder, sämmtlich mit n_1 zum Factor; darauf x_μ andere Glieder, sämmtlich mit n_2 zum Factor u. s. w.: zusammen also, da $\nu+1$ verschiedene n vorhanden sind, $(\nu+1)x_\mu$ verschiedene Glieder. Und da nun die Anzahl der Glieder des Products P_ν durch x_ν zu bezeichnen ist, so ist

$$10. \quad x_\nu = (\nu+1)x_\mu.$$

D. Aus demselben Grunde ist, wenn man die Anzahl der Glieder des Products der $\nu-2$ ersten Reihen in (1.) durch x_λ bezeichnet,

$$11. \quad x_\mu = (\mu+1)x_\lambda,$$

was, in (10.) gesetzt,

$$12. \quad x_\nu = (\nu+1)(\mu+1)x_\lambda$$

giebt. Eben so ergiebt sich $x_\lambda=(\lambda+1)x_\varkappa$ und, in (12.) gesetzt,

$$13. \quad x_\nu = (\nu+1)(\mu+1)(\lambda+1)x_\varkappa;$$

u. s. w. Zuletzt also, da für die erste Reihe allein, $x_\alpha=\alpha+1$ ist,

$$14. \quad x_\nu = (\nu+1)(\mu+1)(\lambda+1)\ldots\ldots(\gamma+1)(\beta+1)(\alpha+1);$$

gemäfs (4.) in (II.).

§. 83.

Lehrsatz.

Wenn man für eine beliebige Zahl z,

$$1. \quad \mathrm{z} = \varepsilon.\mathrm{e}$$

setzt und durch e_φ *jede zu* e *theilerfremde Zahl* >0 *und* $<$ e *bezeichnet, so drückt in*

$$2. \quad \mathrm{x} = \varepsilon.\mathrm{e}_\varphi$$

3. x *alle die Zahlen* 1, 2, 3, 4, ... z

aus, und jede nur einmal, wenn man den ε und e_φ alle die ganzzahligen Werthe beilegt, die sie haben können, 1 und z nicht ausgeschlossen.

Beispiel. Es sei

$$4.\quad z = 126 = 2.3^2.7,$$

so kann e nebst dem zugehörigen ε folgende Werthe haben:

$$5.\quad e = 1,\ 2,\ 3,\ 6,\ 7,\ 9,\ 14,\ 18,\ 21,\ 42,\ 63 \text{ und } 126,$$

$$6.\quad \varepsilon = 126,\ 63,\ 42,\ 21,\ 18,\ 14,\ 9,\ 7,\ 6,\ 3,\ 2 \text{ und } 1.$$

Die zu den verschiedenen e theilerfremden Zahlen e_φ sind folgende:

7.

Für e =	1	2	3	6	7	9	14	18	21	42	63			126		
e_φ =	1	1	1	1	1	1	1	1	1	1	1	22	43	1	43	85
			2	5	2	2	3	5	2	5	2	23	44	5	47	89
					3	4	5	7	4	11	4	25	46	11	53	95
					4	5	9	11	5	13	5	26	47	13	55	97
					5	7	11	13	8	17	8	29	50	17	59	101
					6	8	13	17	10	19	10	31	52	19	61	103
									11	23	11	32	53	23	65	107
									13	25	13	34	55	25	67	109
									16	29	16	37	58	29	71	113
									17	31	17	38	59	31	73	115
									19	37	19	40	61	37	79	121
									20	41	20	41	62	41	83	125.

Multiplicirt man nun nach (2.) diese e_φ mit dem *zugehörigen* ε (6.), so ergiebt sich

8.

Für ε =	126	63	42	21	18	14	9	7	6	3	2			1		
$x = \varepsilon.e_\varphi$ =	126	63	42	21	18	14	9	7	6	3	2	44	86	1	43	85
			84	105	36	28	27	35	12	15	4	46	88	5	47	89
					54	56	45	49	24	33	8	50	92	11	53	95
					72	70	81	77	30	39	10	52	94	13	55	97
					90	98	99	91	48	51	16	58	100	17	59	101
					108	112	117	119	60	57	20	62	104	19	61	103
									66	69	22	64	106	23	65	107
									78	75	26	68	110	25	67	109
									96	87	32	74	116	29	71	113
									102	93	34	76	118	31	73	115
									114	111	38	80	122	37	79	121
									120	123	40	82	124	41	83	125;

und dieses sind, wie man sieht, *alle* die Zahlen 1, 2, 3, 4, ... z, und keine kommt mehr als einmal vor.

Beweis *A*. Es sei n eine der Zahlen 1, 2, 3, 4, ... z (3.). Sie wird *irgend einen* Theiler mit z gemein haben: wenn keinen andern, so den Theiler 1. Welches also auch dieser Theiler sein mag: er ist zugleich ein Theiler von z, und also einer der Werthe von ε.

B. Man nehme den *gröfsten* der Theiler, welchen n und z gemein haben. Er wird immer, als Theiler von z, durch ε bezeichnet.

Alsdann haben aber $\frac{z}{\varepsilon}$ und $\frac{n}{\varepsilon}$ weiter *keinen* Theiler >1 gemein, und sind also zu einander *theilerfremd*, während zugleich $\frac{n}{\varepsilon}>0$ und $<\frac{z}{\varepsilon}$ ist.

C. Aber $\frac{z}{\varepsilon}$ ist vermöge (1.) $=e$, und *alle* zu e *theilerfremden* Zahlen >0 und $<e$ werden durch e_φ bezeichnet. Also ist $\frac{n}{\varepsilon}$ *nothwendig eines der* e_φ.

D. Nun ist identisch

$$9. \quad n = \varepsilon.\frac{n}{\varepsilon},$$

also ist, e_φ statt $\frac{n}{\varepsilon}$ gesetzt,

$$10. \quad n = \varepsilon.e_\varphi = x \ (2.),$$

und daher *kann* x in (2.) *jede* von den Zahlen 1, 2, 3, 4, ... z sein, für irgend ein e und ε. Dieses ist, was zunächst der Lehrsatz behauptet. Es *mufs* aber auch (10.) *alle* x oder n ausdrücken; denn zu *jedem beliebigen* n oder x gehört in (*B*.) irgend ein ε und folglich ein $e=\frac{z}{\varepsilon}$.

E. Gesetzt, *verschiedene* e und ε könnten in (2.) *ein- und dasselbe* x geben, z. B. es könnte

$$11. \quad \varepsilon.e_\varphi = \delta.d_\varphi$$

sein; wo $d>e$ angenommen werden mag.

Da nach (1.) $\varepsilon=\frac{z}{e}$ und $\delta=\frac{z}{d}$ ist, so ist (11.) so viel als

$$12. \quad \frac{z.e_\varphi}{e} = \frac{z.d_\varphi}{d},$$

und daraus folgt

$$13. \quad e_\varphi = \frac{e.d_\varphi}{d}.$$

Dieser Gleichung zufolge müfste also $e.d_\varphi$ mit d *aufgehen*, indem e_φ jedenfalls eine *ganze* Zahl ist. Da d_φ zu d *theilerfremd* ist und also kein Theiler von d in d_φ aufgeht, so müfste d in e *allein* aufgehen. Dies aber ist nicht der Fall, da $d>e$ vorausgesetzt wird. Also kann (13.) und folg-

lich (11.) *nicht* Statt finden: mithin können verschiedene e und ε *nicht* ein- und dasselbe x geben, und folglich drückt $\varepsilon . e_\varphi$ (2.) jedes x aus den Zahlen 1, 2, 3, 4, ... z *nur einmal* aus. Dieses ist die zweite Behauptung des Lehrsatzes.

§. 84.

Lehrsatz.

Die Gesammt-Anzahl der Zahlen, welche zu allen den verschiedenen Theilern einer beliebigen Zahl z (1 *und* z *nicht ausgeschlossen*) *theilerfremd und* >0 *und* $<$ *als je die einzelnen Theiler sind, ist* $=$ z.

Das heifst in Zeichen: wenn man alle die möglichen Theiler einer Zahl z *durch* $e_1, e_2, e_3, \ldots e_n$ *und die Anzahl der zu diesen Theilern theilerfremden Zahlen,* >0 *und* $<$ *als die einzelnen Theiler, durch* $\varphi e_1, \varphi e_2, \varphi e_3, \ldots \varphi e_n$ *bezeichnet, so ist*

$$1. \quad \varphi e_1 + \varphi e_2 + \varphi e_3 + \ldots + \varphi e_n = z.$$

Beispiel. In dem Beispiel zu (§. 83.) sind die e_φ (§. 83. 7.) die zu den verschiedenen möglichen Theilern 1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63 und 126 von $z = 126$ *theilerfremden* Zahlen >0 und $<$ als die Theiler. Ihre *Gesammt-Anzahl* ist $126 = z$.

Erster Beweis. *A.* Nach (§. 83.) erhält man, wenn man die verschiedenen, zu den verschiedenen e theilerfremden Zahlen e_φ mit dem Theiler $\varepsilon = \frac{z}{e}$ von z multiplicirt, *alle* die z Zahlen 1, 2, 3, 4, ... z.

B. Gäbe es nun *mehr* als z verschiedene Zahlen e_φ für die verschiedenen e, so müfste es *entweder* Producte $\varepsilon . e_\varphi$ geben, die *gröfser* als z sind, *oder* es müfsten Producte, die *nicht* gröfser als z sind, *mehr als einmal* vorkommen. *Ersteres* ist nicht der Fall, da e_φ nicht gröfser als e, und $\varepsilon . e = z$, also $\varepsilon . e_\varphi$ *nicht* gröfser als z ist. *Letzteres* ist nach (§. 83.) nicht der Fall, denn $\varepsilon . e_\varphi$ giebt jedes x *nur einmal.* Also kann es *nicht mehr* als z zu den verschiedenen e theilerfremde Zahlen e_φ geben.

C. Gäbe es *weniger* als z Zahlen e_φ, so könnte das Product $\varepsilon . e_\varphi = x$ nicht z verschiedene Werthe haben; denn die e_φ, zu einem und demselben e, sind *nur mit einem* $\varepsilon = \frac{z}{e}$ zu multipliciren. Das Product $x = \varepsilon . e_\varphi$ hat aber nach (§. 83.) wirklich *alle* die z Werthe 1, 2, 3, 4, ... z. Also kann es auch *nicht weniger* als z zu den verschiedenen e theilerfremden Zahlen e_φ >0 und $<e$ geben.

Folglich mufs die Gesammt-Anzahl dieser Zahlen e_φ nothwendig *gleich* z sein; wie es des Lehrsatz behauptet.

Zweiter Beweis. *D.* Es werde nach (§. 21.) z durch

$$2.\quad z = a^{\alpha}.b^{\beta}.c^{\gamma}\ldots m^{\mu}.n^{\nu}$$

ausgedrückt, und bestimmt, dafs $a, b, c, \ldots m, n$ sämmtlich *Stammzahlen* sein sollen. Alsdann wird durch

$$3.\quad e = a^{\alpha_1}.b^{\beta_1}.c^{\gamma_1}\ldots m^{\mu_1}.n^{\nu_1}$$

jeder mögliche Theiler e von z ausgedrückt, wenn man der Reihe nach

$$4.\quad \begin{cases} \alpha_1 = 0, 1, 2, 3, \ldots \alpha, \\ \beta_1 = 0, 1, 2, 3, \ldots \beta, \\ \gamma_1 = 0, 1, 2, 3, \ldots \gamma, \\ \ldots\ldots\ldots\ldots \\ \mu_1 = 0, 1, 2, 3, \ldots \mu, \\ \nu_1 = 0, 1, 2, 3, \ldots \nu \end{cases}$$

setzt. Denn e in (3.) drückt alsdann alle möglichen Potenzen der Stammzahlen $a, b, c, \ldots n$ von 0 an bis $\alpha, \beta, \gamma, \ldots \nu$ und ihre Producte aus; und nur diese und die keiner andern Zahlen gehen in z auf.

E. Nun ist nach (§. 81. 7.) die *Anzahl* der zu e (3.) *theilerfremden* Zahlen > 0 und $< e$:

$$5.\quad \varphi e = a^{\alpha_1-1}(a-1).b^{\beta_1-1}(b-1).c^{\gamma_1-1}(c-1)\ldots m^{\mu_1-1}(m-1).n^{\nu_1-1}(n-1).$$

Giebt man also hier den $\alpha_1, \beta_1, \gamma_1, \ldots \mu_1, \nu_1$ alle die Werthe (4.), so drückt (5.) die *Anzahl* der zu *allen* Theilern e von z *theilerfremden* Zahlen > 0 und $< e$ aus.

F. Dabei ist jedoch zu beobachten, dafs für den Werth *Null* von $\alpha_1, \beta_1, \gamma_1, \ldots \nu_1$ in (5.) für $a^{\alpha_1-1}(a-1)$, $b^{\beta_1-1}(b-1)$ etc. *nicht* $a^{-1}(a-1)$, $b^{-1}(b-1)$ etc. gesetzt werden mufs, sondern blofs 1. Denn wenn z. B. $\alpha_1 = 0$ ist, so ist in (3.) $a^{\alpha_1} = a^0 = 1$ und a ist dann in den hierauf sich beziehenden Theilern e von z (3.) *gar nicht vorhanden*, also auch nicht in φe (5.), und es mufs folglich für $\alpha_1 = 0$ in (5.) statt $a^{\alpha_1-1}(a-1)$ blofs 1 geschrieben werden.

G. Nun bezeichne man die Werthe

$$6.\quad \begin{cases} \text{von } a^{\alpha_1-1}(a-1) \text{ für } \alpha_1 = 0, 1, 2, 3, \ldots \alpha \text{ durch } a_0, a_1, a_2, a_3, \ldots a_\alpha, \\ \text{von } b^{\beta_1-1}(b-1) \text{ für } \beta_1 = 0, 1, 2, 3, \ldots \beta \text{ durch } b_0, b_1, b_2, b_3, \ldots b_\beta, \\ \text{von } c^{\gamma_1-1}(c-1) \text{ für } \gamma_1 = 0, 1, 2, 3, \ldots \gamma \text{ durch } c_0, c_1, c_2, c_3, \ldots c_\gamma, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \text{von } m^{\mu_1-1}(m-1) \text{ für } \mu_1 = 0, 1, 2, 3, \ldots m \text{ durch } m_0, m_1, m_2, m_3, \ldots m_\mu, \\ \text{von } n^{\nu_1-1}(n-1) \text{ für } \nu_1 = 0, 1, 2, 3, \ldots n \text{ durch } n_0, n_1, n_2, n_3, \ldots n_\nu. \end{cases}$$

Alsdann drückt φe (5.) *alle möglichen* Producte von $a_0, a_1, a_2, \ldots a_\alpha$, $b_0, b_1, b_2, \ldots b_\beta$ u. s. w. aus, unter der Bedingung, dafs jedes dieser Producte ein a, ein b, ein c, ..., ein m und ein n, und *nur* eines enthalte.

H. Die *Gesammtheit* oder die Summe aller dieser Producte ist nach (§. 82.), unter der *gleichen* Bedingung,

$$7.\quad \begin{cases} = (a_0 + a_1 + a_2 + a_3 \ldots + a_\alpha) \\ \times (b_0 + b_1 + b_2 + b_3 \ldots + b_\beta) \\ \times (c_0 + c_1 + c_2 + c_3 \ldots + c_\gamma) \\ \ldots\ldots\ldots \\ \times (m_0 + m_1 + m_2 + m_3 \ldots + m_\mu) \\ \times (n_0 + n_1 + n_2 + n_3 \ldots + n_\nu), \end{cases}$$

und dieses ***Product*** ist also die ***Summe*** aller der möglichen Werthe, welche φe (5.) haben kann, mithin die ***Summe der Anzahl*** der zu ***allen möglichen*** Theilern e von z theilerfremden Zahlen > 0 und $< e$, folglich das Nemliche, was in (1.) durch $\varphi e_1 + \varphi e_2 + \varphi e_3 \ldots + \varphi e_n$ bezeichnet wurde.

I. Setzt man nun in den Ausdruck (7.) die Werthe der a, der b, der c u. s. w. aus (6.), mit der Berücksichtigung, dafs nach (*F.*) $a_0 = 1$, $b_0 = 1$, $c_0 = 1$, ... $m_0 = 1$, $n_0 = 1$ ist, so ergiebt sich

$$8.\quad \begin{cases} \varphi e_1 + \varphi e_2 + \varphi e_3 \ldots + \varphi e_n \\ = (1 + (a-1) + a^1(a-1) + a^2(a-1) \ldots + a^{\alpha-1}(a-1)) \\ \times (1 + (b-1) + b^1(b-1) + b^2(b-1) \ldots + b^{\beta-1}(b-1)) \\ \times (1 + (c-1) + c^1(c-1) + c^2(c-1) \ldots + c^{\gamma-1}(c-1)) \\ \ldots\ldots\ldots \\ \times (1 + (m-1) + m^1(m-1) + m^2(m-1) \ldots + m^{\mu-1}(m-1)) \\ \times (1 + (n-1) + n^1(n-1) + n^2(n-1) \ldots + n^{\nu-1}(n-1)). \end{cases}$$

K. Es ist aber z. B. die *erste* Reihe rechts in (8.)

$$9.\quad \begin{cases} 1 + (a-1) + a(a-1) + a^2(a-1) \ldots + a^{\alpha-2}(a-1) + a^{\alpha-1}(a-1) \\ = 1 + a + a^2 + a^3 \ldots + a^{\alpha-1} + a^\alpha \\ \quad - 1 - a - a^2 - a^3 \ldots - a^{\alpha-1} \\ = a^\alpha. \end{cases}$$

Auf dieselbe Weise ist die *zweite* Reihe rechts in (8.) $= b^\beta$, die dritte $= c^\gamma$ u. s. w. Also giebt (8.)

$$10.\quad \varphi e_1 + \varphi e_2 + \varphi e_3 \ldots + \varphi e_n = a^\alpha . b^\beta . c^\gamma \ldots m^\mu . n^\nu;$$

und vermöge (2.)

$$11.\quad \varphi e_1 + \varphi e_2 + \varphi e_3 \ldots + \varphi e_n = z;$$

gemäfs (1.) im Lehrsatz.

Dritter Beweis. *K.* Man berücksichtige zuerst den *einzigen* Theiler

12. $\varepsilon = b^{\beta_1}.c^{\gamma_1}\dots m^{\mu_1}.n^{\nu_1}$

von z in (3.), für einen *festen, bestimmten* Werth der Exponenten $\beta_1, \gamma_1, \dots \mu_1, \nu_1$: so ist die Anzahl der zu demselben theilerfremden Zahlen > 0 und $< \varepsilon$ nach (5.)

13. $\varphi\varepsilon = b^{\beta_1-1}(b-1).c^{\gamma_1-1}(c-1)\dots m^{\mu_1-1}(m-1).n^{\nu_1-1}(n-1)$.

L. Nun erhalte dieser Theiler ε noch den Factor a, so ist nach (5.)

14. $\varphi(\varepsilon a) = (a-1).b^{\beta_1-1}(b-1).c^{\gamma_1-1}(c-1)\dots m^{\mu_1-1}(m-1).n^{\nu_1-1}(n-1)$
$= (a-1)\varphi\varepsilon.$

Bekommt der Theiler ε statt a den Factor a^2, so ist nach (5.)

15. $\varphi(\varepsilon a^2) = a(a-1).b^{\beta_1-1}(b-1).c^{\gamma_1-1}(c-1)\dots m^{\mu_1-1}(m-1).n^{\nu_1-1}(n-1)$
$= a(a-1)\varphi\varepsilon.$

Bekommt ε den Factor a^3, so ist nach (5.)

16. $\varphi(\varepsilon a^3) = a^2(a-1).b^{\beta_1-1}(b-1).c^{\gamma_1-1}(c-1)\dots m^{\mu_1-1}(m-1).n^{\nu_1-1}(n-1)$
$= a^2(a-1)\varphi\varepsilon.$

Setzt man so weiter dem Theiler ε der Reihe nach die Factoren $a^4, a^5, a^6, \dots a^\alpha$ zu, immer für *einen und denselben bestimmten* Werth der Exponenten $\beta_1, \gamma_1, \delta_1, \dots \mu_1, \nu_1$, so ergiebt sich aus (13. 14. 15. etc.) zusammen für die *Summe* der Anzahl der theilerfremden Zahlen zu allen *denjenigen* Theilern ε von z (3.), welche *sämmtlich* den *einen bestimmten* Factor $b^{\beta_1}.c^{\gamma_1}\dots m^{\mu_1}.n^{\nu_1}$ und dabei der Reihe nach noch die Factoren $a^0, a^1, a^2, a^3, \dots a^\alpha$ haben,

17. $$\begin{cases} \varphi\varepsilon + \varphi(\varepsilon a) + \varphi(\varepsilon a^2) + \varphi(\varepsilon a^3)\dots + \varphi(\varepsilon a^\alpha) \\ = [1 + a - 1 + a(a-1) + a^2(a-1) + a^3(a-1)\dots + a^{\alpha-2}(a-1) + a^{\alpha-1}(a-1)]\varphi\varepsilon \\ = \begin{Bmatrix} 1 + a + a^2 + a^3 + a^4\dots + a^{\alpha-1} + a^\alpha \\ -1 - a - a^2 - a^3 - a^4\dots - a^{\alpha-1} \end{Bmatrix}\varphi\varepsilon \\ = a^\alpha.\varphi\varepsilon. \end{cases}$$

M. Für *jeden* der Theiler

18. $\varepsilon = b^{\beta_1}.c^{\gamma_1}\dots m^{\mu_1}.n^{\nu_1}$

von z, für einen *festen bestimmten* Werth von $\beta_1, \gamma_1, \dots \mu_1, \nu_1$ beträgt also, wenn man dem ε der Reihe nach die Factoren $a^0, a^1, a^2, \dots a^\alpha$ hinzufügt, die Summe der alsdann zu diesen *verschiedenen* Theilern von z theilerfremden Zahlen das a^α*fache* der Anzahl $\varphi\varepsilon$ der zu ε *selbst* theilerfremden Zahlen.

N. Dieses gilt nun gleichmäfsig von *jedem* der Theiler ε (12.), die man erhält, wenn man den $\beta_1, \gamma_1, \dots \mu_1, \nu_1$ immer *andere,* und alle diejenigen Werthe (3.) beilegt, welche sie haben können. Immer ist für jedes ε

die Zahl $\varphi\varepsilon$ der zu ihm theilerfremden Zahlen a^α mal so grofs, so wie man dem ε nach der Reihe nach alle die Factoren $a^0, a^1, a^2, a^3, \ldots a^\alpha$ zusetzt. Also, da das *Gleiche* von *jedem* ε und seinem $\varphi\varepsilon$ gilt, so gilt es auch von der *Summe* der $\varphi\varepsilon$, die durch $S\varphi\varepsilon$ bezeichnet werden mag.

O. Man erhält aber, wenn man allen den möglichen Werthen, die ε (12.) haben kann, *jedem* noch die Factoren $a^0, a^1, a^2, \ldots a^\alpha$ zusetzt, *alle möglichen* Werthe, *die e in* (3.) *haben kann*, also *alle möglichen* Theiler von z.

Daraus folgt, dafs sich, wenn man $S\varphi\varepsilon$ mit a^α *multiplicirt*, die Summe der Anzahl der zu *allen möglichen Theilern von z* theilerfremden Zahlen, welche durch $S\varphi e$ zu bezeichnen ist, ergeben mufs. Und folglich ist

$$19. \quad S\varphi e = a^\alpha S\varphi\varepsilon.$$

P. So wie nun, wenn man von den e (3.) erst a ausschliefst, e dadurch auf ε (18.) reducirend, $S\varphi e = a^\alpha S\varphi\varepsilon$ ist (19.), so ist auch nothwendig, wenn man von den ε (12.) b ausschliefst und das dadurch reducirte ε etwa durch ε_1 bezeichnet,

$$20. \quad S\varphi\varepsilon = b^\beta S\varphi\varepsilon_1;$$

und weiter, wenn man von den ε_1, c ausschliefst und ε_2 statt ε_1 schreibt, ferner d von ε_2, und ε_3 statt ε_2 schreibt u. s. w.

$$21. \quad \begin{cases} S\varphi\varepsilon_1 = c^\gamma S\varphi\varepsilon_2, \\ S\varphi\varepsilon_2 = d^\delta S\varphi\varepsilon_3, \\ \cdots\cdots\cdots\cdots \\ S\varphi\varepsilon_{\mu-2} = m^\mu S\varphi\varepsilon_{\mu-1}. \end{cases}$$

Dieses giebt, (21.) in einander, dann in (20.) und dies zuletzt in (19.) substituirt,

$$22. \quad S\varphi e = a^\alpha . b^\beta . c^\gamma . d^\delta \ldots m^\mu S\varphi\varepsilon_{\mu-1}.$$

Q. Nachdem $a, b, c, d, \ldots m$ in e (3.) ausgeschlossen sind, bleibt aber für $\varepsilon_{\mu-1}$ blofs noch n^ν übrig, und die Summe $S\varphi\varepsilon_{\mu-1}$ der $S\varphi n^{\nu_1}$, der Anzahl der zu den verschiedenen Theilern $n^0, n^1, n^2, n^3, \ldots n^\nu$ von n^ν theilerfremden Zahlen ist nach (5.)

$$23. \quad \begin{cases} 1 + n - 1 + n(n-1) + n^2(n-1) + n^3(n-1) \ldots + n^{\nu-2}(n-1) + n^{\nu-1}(n-1) \\ \quad = 1 + n + n^2 + n^3 \ldots + n^{\nu-1} + n^\nu \\ \quad - 1 - n - n^2 + n^3 \ldots - n^{\nu-1} \\ \quad = n^\nu; \end{cases}$$

also ist schliefslich in (22.)

$$24. \quad S\varphi e = a^\alpha . b^\beta . c^\gamma . d^\delta \ldots m^\mu . n^\nu,$$

und dies giebt vermöge (2.)

$$25. \quad S\varphi e = z;$$

das heifst: die Summe der Anzahl der zu allen möglichen Theilern e von z theilerfremden Zahlen ist $= z$; wie es der Lehrsatz behauptet.

Anm. 1. *R.* Der *zweite* Beweis bedarf des Satzes (§. 81.), mit seinem Vorgänger (§. 78.) und den Vorgängern (§. 74. 75. 76. und 77.) von diesem; auch aufserdem noch des Satzes (§. 82.). Der *dritte* Beweis bedarf zwar (§. 82.) nicht, aber eben so der übrigen. Der *erste* Beweis dagegen bedarf *blofs* des Satzes (§. 83.) und dürfte daher der einfachste und am besten für die Elemente geeignet sein.

Anm. 2. *S.* Nach (§. 63.) ist für jede *Stammzahl* p die Anzahl der Stammwurzeln für einen beliebigen Theiler δ von $p-1$, 1 und $p-1$ selbst eingeschlossen, der Anzahl der zu δ *theilerfremden* Zahlen gleich; zu jedem andern Theiler δ gehören andere Stammwurzeln, und alle zusammen sind die sämmtlichen Zahlen 1, 2, 3, 4, ... $p-1$, und jede nur einmal. Darin liegt also ebenfalls ein Beweis, dafs die Summe der Anzahl der zu allen verschiedenen Theilern von $p-1$ theilerfremden Zahlen der Zahl $p-1$ selbst gleich ist. Aber dieser Beweis pafst *nur* auf Zahlen $p-1$, für welche p eine *Stammzahl* ist: die obigen Beweise gelten allgemein für *jede beliebige* Zahl z.

§. 85.

Lehrsatz.

I. *Wenn in der Gleichung*

$$1. \quad u.v = \mathfrak{G}z + w$$

u, v *und* w *ganze Zahlen, und zwei davon, gleichviel welche, zu der ganzen Zahl* z *theilerfremd sind, so ist es auch die dritte, es mögen jene zwei ungleich, oder gleich, und zu einander theilerfremd sein, oder nicht.*

II. *Wenn in der Gleichung* (1.) *eine der drei Zahlen* u, v *und* w, *gleichviel welche, alle zu* z *theilerfremden Zahlen* >0 *und* $<z$ *durchläuft (die, wie weiter oben, durch* z_φ *bezeichnet werden mögen und ihre Anzahl durch* φz, *oder auch, kürzer, blofs durch* φ), *während eine zweite der drei Zahlen, gleichviel welche, stets denselben Werth behält, so durchläuft die dritte ebenfalls alle zu* z *theilerfremden Zahlen* $z_\varphi > 0$ *und* $z_\varphi < z$, *obwohl in verschiedener Ordnung.*

Beispiel. Es sei

$$2. \quad z = 15.$$

Alsdann sind die zu z *theilerfremden* Zahlen >0 und $<z$ folgende:

$$3. \quad z_\varphi = 1, 2, 4, 7, 8, 11, 13 \text{ und } 14.$$

Zu I. Es sei z. B. in (1.) $u=7$, $v=11$, so giebt (1.) $7.11=5.z+2$, also $w=2$; welches ebenfalls eines der z_φ ist. Es sei $u=4$, $w=13$, so ist $4.7=1.15+13$, also $v=7$; wiederum eines der z_φ. Es sei $v=11$, $w=4$, so ist $14.11=10.15+4$, also $u=14$; ebenfalls eines der z_φ.

Zu II. *a.* Läfst man u oder v *denselben* Werth, z. B. 4, behalten, während v oder u alle z_φ durchläuft, welche beiden Fälle offenbar nur einer sind, da die Factoren u und v vertauscht werden können, so findet sich

$$4. \left\{\begin{array}{l} 4.\ 1 = \mathfrak{G}z+\ 4, \text{ also } w = 4, \\ 4.\ 2 = \mathfrak{G}z+\ 8, \quad - \ - \ - \ 8, \\ 4.\ 4 = \mathfrak{G}z+\ 1, \quad - \ - \ - \ 1, \\ 4.\ 7 = \mathfrak{G}z+13, \quad - \ - \ - \ 13, \\ 4.\ 8 = \mathfrak{G}z+\ 2, \quad - \ - \ - \ 2, \\ 4.11 = \mathfrak{G}z+14, \quad - \ - \ - \ 14, \\ 4.13 = \mathfrak{G}z+\ 7, \quad - \ - \ - \ 7, \\ 4.14 = \mathfrak{G}z+11, \quad - \ - \ - \ 11. \end{array}\right\} \text{ Also durchläuft } w \text{ ebenfalls alle } z_\varphi.$$

b. Läfst man w *denselben* Werth, z. B. 4 oder 11, behalten und dagegen v oder u alle z_φ durchlaufen, welche beide Fälle wieder nur einer sind, indem die unverändert bleibende Zahl ebensowohl durch u als durch v bezeichnet werden kann, so findet sich

$$5. \left\{\begin{array}{l} 1.\ 4 = \mathfrak{G}z+4 \\ 2.\ 2 = \mathfrak{G}z+4 \\ 4.\ 1 = \mathfrak{G}z+4 \\ 7.\ 7 = \mathfrak{G}z+4 \\ 8.\ 8 = \mathfrak{G}z+4 \\ 11.14 = \mathfrak{G}z+4 \\ 13.13 = \mathfrak{G}z+4 \\ 14.11 = \mathfrak{G}z+4 \end{array}\right\} \text{ für } w=4, \quad 6. \left\{\begin{array}{l} 1.11 = \mathfrak{G}z+11 \\ 2.13 = \mathfrak{G}z+11 \\ 4.14 = \mathfrak{G}z+11 \\ 7.\ 8 = \mathfrak{G}z+11 \\ 8.\ 7 = \mathfrak{G}z+11 \\ 11.\ 1 = \mathfrak{G}z+11 \\ 13.\ 2 = \mathfrak{G}z+11 \\ 14.\ 4 = \mathfrak{G}z+11 \end{array}\right\} \text{ für } w=11.$$

Also durchläuft, wie man sieht, v für ein *unverändertes* w alle z_φ, wenn es mit u geschieht.

c. Läfst man u oder v denselben Werth, z. B. 8, behalten, während w alle z_φ durchläuft, welche beiden Fälle wiederum nur einer sind, indem die unverändert bleibende Zahl ebensowohl durch u als durch v bezeichnet werden kann, so findet sich

$$7.\quad \left\{\begin{aligned} 8.\ 2 &= \mathfrak{G}z+1,\\ 8.\ 4 &= \mathfrak{G}z+2,\\ 8.\ 8 &= \mathfrak{G}z+4,\\ 8.14 &= \mathfrak{G}z+7,\\ 8.\ 1 &= \mathfrak{G}z+8,\\ 8.\ 7 &= \mathfrak{G}z+11,\\ 8.11 &= \mathfrak{G}z+13,\\ 8.13 &= \mathfrak{G}z+14. \end{aligned}\right.$$

Während also w alle z_φ durchläuft und u *denselben* Werth behält, durchläuft auch v alle z_φ.

Beweis von I. *Erstlich A.* Wäre, wenn zuerst u und v zu z *theilerfremd* sind, w *nicht* zu z theilerfremd, sondern hätte mit z irgend einen *Stammtheiler* $\delta > 1$ gemein, so müfste δ nach (§. 18.), da es in $\mathfrak{G}z$ und w aufgehen soll, auch in $u.v$ aufgehen; also *entweder* in u, *oder* in v; denn die *Stammzahl* δ ist untheilbar. Aber weder u noch v hat nach der Voraussetzung irgend einen Stammtheiler > 1 mit z gemein: also geht δ *nicht* in $u.v$ auf; und folglich kann w mit z *keinen* Stammtheiler $\delta > 1$ gemein haben und ist demnach zu z nothwendig *theilerfremd.*

Zweitens B. Wäre, wenn zweitens u und w zu z *theilerfremd* sind, v *nicht* zu z theilerfremd, sondern hätte mit z irgend einen *Stammtheiler* $\delta > 1$ gemein, so müfste δ, da es in $u.v$ und $\mathfrak{G}z$ aufgehen soll, nach (§. 18.) auch in w aufgehen, und w und z wären also *nicht* zu einander theilerfremd; gegen die Voraussetzung. Also können v und z keinen Theiler $\delta > 1$ gemein haben und sind folglich nothwendig zu einander *theilerfremd.*

Drittens C. Ganz wie in (*B.*) verhält es sich aus *demselben* Grunde, drittens, mit u und z, wenn v und w zu z theilerfremd sind.

Beweis von II. *Erstlich D.* *a.* Es behalte u stets *denselben* Werth, während v *alle* z_φ durchläuft: so entstehen φz, oder kürzer, φ Werthe von w, und alle diese Werthe sind nach (I.) zu z *theilerfremd.*

b. Wären nun zwei Werthe von w, z. B. w_1 und w_2, für zwei *verschiedene* Werthe v_1 und v_2 von v *einander gleich*, so müfste

$$8.\quad uv_1 = \mathfrak{G}z + w_1 \quad\text{und}\quad uv_2 = \mathfrak{G}z + w_2,$$

und wegen $w_1 = w_2$,

$$9.\quad u(v_1 - v_2) = \mathfrak{G}z$$

sein, also $u(v_1 - v_2)$ mit z *aufgehen.* Aber u hat nach der Voraussetzung *keinen* Theiler mit z gemein: also müfste z in $v_1 - v_2$ allein aufgehen. Dies

ist nicht möglich, da v_1 und v_2 *beide* $< z$ sind und also $v_1 - v_2$ um so mehr $< z$ ist. Folglich geht z in $u(v_1 - v_2)$ *nicht* auf, und folglich können nicht zwei Werthe von w einander gleich sein.

c. Nun sind ihrer φz oder φ, und *alle* sind zu z *theilerfremd* (*a.*). Also durchläuft w nothwendig *alle* zu z theilerfremden Zahlen $z_\varphi > 0$ und $< z$.

Zweitens E. Der Fall, wenn v stets denselben Werth behält, während u alle z_φ durchläuft, ist nur der vorige, indem der unverändert bleibende Werth ebensowohl durch v als durch u bezeichnet werden kann.

Drittens F. Es behalte w stets *denselben* Werth, während u alle z_φ durchläuft.

a. Zuerst folgt aus (*D.*), daſs es, welchen Werth auch w mag haben sollen, zu *jedem* u nothwendig ein v giebt, welches die Gleichung (1.) erfüllt. Denn wenn u *irgend einen* der Werthe z_φ hat, und v durchläuft *alle* z_φ, so durchläuft nach (*D.*) auch w alle z_φ, und folglich werden von w für jedes beliebige u durch die verschiedenen Werthe von v *alle* z_φ berührt, folglich auch *derjenige bleibende* Werth von w, welchen man ihm zugetheilt hat, durch irgend ein v für ein bestimmtes u. Mithin giebt es für jedes u nothwendig irgend ein v, für welches w den *bestimmten* bleibenden Werth bekommt

b. Durchliefe nun v für ein- und dasselbe w nicht *alle* z_φ, während u alle diese Werthe annimmt, so müſsten zwei verschiedene u, z. B. u_1 und u_2, mit *demselben* v *dasselbe* w geben, also müſste

10. $u_1 . v = \mathfrak{G} z + w$ und $u_2 . v = \mathfrak{G} z + w$

und folglich

11. $(u_1 - u_2) v = \mathfrak{G} z$

sein, und mithin $(u_1 - u_2) v$ mit z *aufgehen.* Dieses ist aus ganz gleichen Gründen wie in (*D. b.*) nicht möglich. Also kann mit zwei *verschiedenen* u *nicht dasselbe* v *dasselbe* w geben, und folglich muſs, wenn w stets denselben Werth behält, während u *alle* z_φ durchläuft, auch nothwendig v *alle* z_φ durchlaufen.

Viertens G. Der Fall, wenn w stets denselben Werth behält, während v alle z_φ durchläuft, ist nur der vorige, indem diejenige Zahl, welche alle z_φ durchlaufen *soll,* worauf dann, wie sich fand, die andere alle z_φ durchlaufen *muſs,* ebensowohl durch v als durch u bezeichnet werden kann.

Fünftens H. Es behalte u stets *denselben* Werth, während w alle z_φ durchläuft.

a. Zuerst folgt aus (*D.*), dafs es, welchen Werth auch u mag haben sollen, zu jedem w nothwendig ein v giebt, welches die Gleichung (1.) erfüllt. Denn wenn u einen bestimmten Werth hat, und v durchläuft *alle* z_φ, so durchläuft w nach (*D.*) ebenfalls *alle* z_φ. Also *jeder* Werth, den w *soll* haben können, wird für jeden *bestimmten* Werth von u durch irgend ein v berührt. Mithin giebt es für jeden *bestimmten* und bleibenden Werth von u, und für *jeden* Werth, den w bekommen kann, ein zugehöriges v.

b. Durchliefe nun v für ein- und dasselbe u nicht *alle* z_φ, während w alle z_φ durchläuft, so müfste v für zwei *verschiedene* Werthe von w, z. B. w_1 und w_2, und für *dasselbe* u, *denselben* Werth haben können, also müfste

$$12. \quad uv = \mathfrak{G}z + w_1 \quad \text{und} \quad uv = \mathfrak{G}z + w_2,$$

folglich

$$13. \quad 0 = \mathfrak{G}z + w_1 - w_2 \quad \text{oder} \quad w_1 - w_2 = \mathfrak{G}z$$

sein und mithin $w_1 - w_2$ mit z *aufgehen*. Dieses ist nicht möglich, da w_1 und w_2 beide $< z$ sind und also $w_1 - w_2$ um so mehr $< z$ ist. Also kann v für zwei *verschiedene* w und ein- und dasselbe u *nicht gleiche* Werthe haben. Und folglich mufs v, wenn w für einen und denselben Werth von u alle z_φ durchläuft, ebenfalls *alle* z_φ durchlaufen.

Sechstens I. Der Fall, wenn v *denselben* Werth behält, während w alle z_φ durchläuft, ist wieder nur der vorige, indem diejenige Zahl, welche denselben Werth behalten *soll*, während w alle z_φ durchläuft, wobei dann, wie sich findet, die andere alle z_φ durchlaufen *mufs*, ebensowohl durch v als durch u bezeichnet werden kann.

§. 86.

Lehrsatz.

Wenn in

$$1. \quad a^\alpha b^\beta c^\gamma \ldots n^\nu = \mathfrak{G}z + r,$$

wo $\alpha, \beta, \gamma, \ldots \nu$ *beliebige ganze positive Zahlen bezeichnen,* a, b, c, ... n *sämmtlich einzeln zu* z *theilerfremd sind, so ist es auch* r; *gleichviel ob* a, b, c, ... n *unter sich theilerfremd sind, oder nicht.*

Beispiel. Es sei $a=4$, $b=6$, $c=15$, $\alpha=5$, $\beta=3$, $\gamma=2$, $z=91$, so ist

$$2. \quad a^\alpha b^\beta c^\gamma = 4^5.6^3.15^2 = 256.216.225 = 12441600 = 136721.z + 39$$

und $r=39$ hat mit $z=91$ keinen Theiler >1 gemein.

Beweis. Hätte r mit z irgend einen Theiler $\delta > 1$ gemein, so müfste derselbe nach (§. 18.) in irgend einen der Factoren $a, a, a, \ldots b, b, \ldots$

$c, c, \ldots$ von z, oder in mehrere von ihnen aufgehen, und also hätten dann diese Factoren mit z den Theiler $\delta > 1$ gemein und wären also zu z nicht theilerfremd. Dieses ist der Voraussetzung entgegen, und folglich kann r zu z nur theilerfremd sein.

§. 87.

Lehrsatz.

Für jede, zu einer beliebigen Zahl z theilerfremde Zahl $u = z_\varphi$ ***ist, wenn man die Anzahl derjenigen dieser Zahlen*** z_φ***, welche*** $< z$ ***sind, wie oben durch*** φz ***oder auch kürzer durch*** φ ***bezeichnet,***

$$1. \quad u^{\varphi z} \text{ oder } u^{\varphi} = \mathfrak{G} z + 1.$$

Die Zahl u ***kann nach Belieben kleiner, oder gröſser als*** z, ***und sowohl positiv als negativ sein.***

Dieser Satz ist eine Verallgemeinerung des Fermatschen Lehrsatzes (§. 40.) ***und kann deshalb „Verallgemeinerter Fermatscher Lehrsatz" heiſsen.***

Beispiel. Es sei

$$2. \quad z = 15,$$

so hat $u = z_\varphi$ folgende φz oder $\varphi = 8$ Werthe:

$$3. \quad u = z_\varphi = 1, 2, 4, 7, 8, 11, 13 \text{ und } 14$$

Dieselben geben, der Reihe nach in (1.), statt u gesetzt,

$$4. \quad \begin{cases} 1^8 = \mathfrak{G} z + 1, \\ 2^8 = 256 = \mathfrak{G} z + 1, \\ 4^8 = 2^{16} = (\mathfrak{G} z + 1)^2 = \mathfrak{G} z + 1, \\ 7^8 = 49^4 = (\mathfrak{G} z + 4)^4 = \mathfrak{G} z + 256 = \mathfrak{G} z + 1, \\ 8^8 = 4^{16} = (\mathfrak{G} z + 1)^2 = \mathfrak{G} z + 1, \\ 11^8 = 121^4 = (\mathfrak{G} z + 1)^4 = \mathfrak{G} z + 1, \\ 13^8 = (\mathfrak{G} z - 2)^8 = (\mathfrak{G} z + 2)^8 = \mathfrak{G} z + 1, \\ 14^8 = (\mathfrak{G} z - 1)^8 = \mathfrak{G} z + 1. \end{cases}$$

Alle z_φ also geben, auf die $\varphi z = \varphi = 8$te Potenz erhoben, $\mathfrak{G} z + 1$.

Auch für jedes $u > 15$, welches zu 15 theilerfremd ist, ist $u^8 = \mathfrak{G} z + 1$. Z. B. $u = 52$ giebt

$$5. \quad 52^8 = (\mathfrak{G} z + 7)^8 = \mathfrak{G} z + 7^8 = \mathfrak{G} z + 1 \quad (4.).$$

Desgleichen ist z. B. für das *negative* $u = -34$,

$$6. \quad (-34)^8 = (-3.z + 11)^8 = (\mathfrak{G} z + 11)^8 = \mathfrak{G} z + 11^8 = \mathfrak{G} z + 1 \quad (4.).$$

Beweis. *A.* Es sei u irgend ein *bestimmtes* z_φ und

$$7. \quad uv = \mathfrak{G} z + w.$$

Läfst man in dieser Gleichung v *alle* die Werthe von z_φ durchlaufen, so durchläuft nach (§. 85. II.) auch w *alle* z_φ; obwohl in verschiedener Ordnung.

B. Bezeichnet man also der Reihe nach die φz Werthe, welche v bekommen kann, durch $v_1, v_2, v_3, \ldots . v_{\varphi z}$, und die in (7.) *zugehörigen* Werthe von w durch $w_1, w_2, w_3, \ldots . w_{\varphi z}$, so ergiebt sich

$$8. \quad \begin{cases} uv_1 = \mathfrak{G}z + w_1, \\ uv_2 = \mathfrak{G}z + w_2, \\ uv_3 = \mathfrak{G}z + w_3, \\ \ldots\ldots\ldots\ldots \\ uv_{\varphi z} = \mathfrak{G}z + w_{\varphi z}. \end{cases}$$

C. Multiplicirt man die sämmtlichen Gleichungen (8.), φz an der Zahl, in einander, so erhält man

$$9. \quad u^{\varphi z}.v_1 v_2 v_3 \ldots . v_{\varphi z} = \mathfrak{G}z + w_1 w_2 w_3 \ldots . w_{\varphi z}.$$

Aber die w haben zusammengenommen *dieselben* Werthe wie die v, nur in verschiedener Aufeinanderfolge; denn sowohl die w als die v sind die *sämmtlichen* z_φ: also ist das *Product*

$$10. \quad v_1 v_2 v_3 \ldots . v_{\varphi z} = w_1 w_2 w_3 \ldots . w_{\varphi z},$$

und folglich in (9.)

$$11. \quad u^{\varphi z}.v_1 v_2 v_3 \ldots . v_{\varphi z} = \mathfrak{G}z + v_1 v_2 v_3 \ldots . v_{\varphi z},$$

und hieraus folgt

$$12. \quad v_1 v_2 v_3 \ldots . v_{\varphi z}(u^{\varphi z} - 1) = \mathfrak{G}z:$$

mithin mufs $v_1 v_2 v_3 \ldots . v_{\varphi z}(u^{\varphi z} - 1)$ mit z *aufgehen.*

D. Aber *keiner* der Factoren v hat mit z irgend einen Stammtheiler $\delta > 1$ gemein, denn alle sind zu z *theilerfremd:* also geht auch das Product $v_1 v_2 v_3 \ldots . v_{\varphi z}$ mit δ nicht auf, und folglich auch nicht mit z, noch mit irgend einem Factor von z. Mithin mufs $u^{\varphi z} - 1$ *allein* mit z aufgehen und folglich

$$13. \quad u^{\varphi z} - 1 = \mathfrak{G}z \quad \text{oder} \quad u^{\varphi z} = \mathfrak{G}z + 1$$

sein; wie es der Lehrsatz in (1.) behauptet.

E. Ist u *gröfser* als z, also

$$14. \quad u = \mathfrak{G}z + u_1,$$

wo nun $u_1 < z$, so ist nothwendig, wenn u zu z *theilerfremd* ist, auch u_1 zu z *theilerfremd.* Denn hätte u_1 und z einen Theiler $\delta > 1$ gemein, so müfste derselbe nach (§. 18.) in u aufgehen und u und z wären dann *nicht* theilerfremd; gegen die Voraussetzung. Also ist u_1 in (14.) nothwendig *irgend eines der* $z_\varphi < z$.

Nun giebt (14.)

$$15. \quad u^{\varphi z} = (\mathfrak{G}z + u_1)^{\varphi z} = \mathfrak{G}z + u_1^{\varphi z}.$$

Aber für jedes $u_1 = z_\varphi < z$ ist nach (1.) $u_1^{\varphi z} = \mathfrak{G}z + 1$. Also ist auch in (15.)

$$16. \quad u^{\varphi z} = \mathfrak{G}z + \mathfrak{G}z + 1 = \mathfrak{G}z + 1;$$

das heifst: auch für *positive u*, welche $> z$ und zu z theilerfremd sind, gilt der Lehrsatz.

F. Ist u *negativ* und sein zeichenfreier Werth $< z$ oder $> z$, aber zu z *theilerfremd*, so läfst sich $\mathfrak{G}$ immer so annehmen, dafs

$$17. \quad u = \mathfrak{G}z + u_1$$

ist, wo $u_1 < z$ und > 0 und also eines der z_φ ist, und es folgt dann, eben wie in (*E.*), dafs der Lehrsatz auch für *diese u* gilt.

§. 88.

Zweiter Beweis des *Fermat*schen Lehrsatzes (§. 40.).

A. Wenn in (§. 87.) z eine *Stammzahl* p ist, so sind alle die Zahlen 1, 2, 3, 4, ... $p-1$ zu $z = p$ *theilerfremd*, und folglich kann in (§. 87.) u alle die Werthe

$$1. \quad u = 1, 2, 3, 4, \ldots\ldots p-1$$

haben. Die Anzahl φz oder φ dieser Werthe von u ist $p-1$: also giebt (§. 87. 1.) in dem Falle $z = p$:

$$2. \quad u^{p-1} = \mathfrak{G}p + 1;$$

dem Satze (§. 40.) gemäfs.

Anmerk. *B.* Der *verallgemeinerte Fermat*sche Satz (§. 87.) bedarf *nur* des einfachen Satzes (§. 85.), sogar nur des *einen* Falles desselben, wenn u *denselben* Werth behält und v alle z_φ durchläuft. Also könnte man in den Elementen auch recht gut den *Fermat*schen Satz sogleich in seiner verallgemeinerten Form (§. 87.) aufstellen und den eigentlich sogenannten *Fermat*schen Satz, für den Fall, wenn z eine *Stammzahl* p ist, auf die Weise wie in dem gegenwärtigen Paragraph, als einen einzelnen besondern Fall daraus ableiten.

§. 89.

Erklärung.

A. Wir haben in (§. 45.), wenn in der Gleichung

$$1. \quad u^2 = \mathfrak{G}p + r$$

p eine *Stammzahl* ist, die Reste r zu einem beliebigen u *Quadratreste zu p* genannt, und diejenigen Zahlen > 0 und $< p$, welche zu *keinem u* gehören, *Nichtquadratreste zu p*.

In (§. 46.) haben wir für die Gleichung

$$2.\quad uv = \mathfrak{G}z + w$$

die Zahlenpaare u und v, welche für *dasselbe z gleiche w* geben, *zusammengehörige Zahlen für w zu z* genannt.

Es mag jetzt die Bedeutung dieser Benennungen auf folgende Art *erweitert* werden.

B. a. Es soll allgemein, aber immer für Zahlen u und v, die zu einer beliebigen Zahl z *theilerfremd* und $< z$ sind, jedes Zahlenpaar u und v in der Gleichung (2.), auch dann, wenn nicht mehrere Paare dasselbe w geben, *zusammengehörige Zahlen für w* zu z heifsen.

b. Sind u und v einander *gleich*, so dafs in (2.)

$$3.\quad u^2 = \mathfrak{G}z + w$$

ist, so soll w *Quadratrest zu z* heifsen; auch wenn z nicht eine Stammzahl ist.

c. Sind u und v *nicht* einander gleich, so soll in (2.) w *Nichtquadratrest zu z* heifsen.

d. Das Product uv soll, je nachdem u und v gleich, oder ungleich sind, *Quadrat* oder *Nichtquadrat für z zu w* heifsen.

e. Die Zahlen u und v selbst sollen, wenn sie einander gleich sind, wie in (3.), *Quadratwurzeln* zu w für z heifsen und, sind sie ungleich, wie in (2.), *Factoren zu w für z.*

§. 90.

Lehrsatz.

I. *Die Anzahl derjenigen Paare zu einer beliebigen Zahl* z *theilerfremden ungleichen Zahlen* u *und* v $<$ z, *welche in der Gleichung*

$$1.\quad \mathrm{uv} = \mathfrak{G}\mathrm{z} + \mathrm{w}$$

den nemlichen Werthe von w *geben, also, nach* (§. 89.) *ausgedrückt, die Anzahl der Nichtquadrate zu gleichem* w *für* z, *ist immer gerade.*

II. *Jedes der Nichtquadrate zu gleichen* w *für* z *in* (1.) *kommt für alle die Werthe* $\mathrm{z}_\varphi < \mathrm{z}$, *welche* u *und* v *darin haben können, zweimal vor; und schon in der Hälfte dieser Nichtquadrate kommen alle Werthe vor, welche* u *und* v *in den Nichtquadraten haben können, und jeder nur einmal.*

II. *Die Anzahl der Quadrate für* z *zu gleichen* w, *also z. B. der* x *in*

$$2.\quad \mathrm{x}^2 = \mathfrak{G}\mathrm{z} + \mathrm{w}$$

für ein- und dasselbe w, *ist ebenfalls immer gerade; den Fall* $z = 2$ *allein ausgenommen.*

IV. *Zu jeder Quadratwurzel* x_1 *zu* w *für* z *gehört eine zweite* $x_2 = z - x_1$, *welche mit* x *multiplicirt den Rest* —w *zu* z *giebt. Also wenn z. B.*

$$3.\quad x_1^2 = \mathfrak{G}z + w \quad \textit{und} \quad x_2^2 = \mathfrak{G}z + w$$

ist, so ist

$$4.\quad x_1 x_2 = \mathfrak{G}z - w.$$

V. *Die Quadrate und die Nichtquadrate zu einem und demselben* w *haben immer verschiedene Factoren. Das heifst, wenn z. B.*

$$5.\quad x^2 = \mathfrak{G}z + w,$$

und zugleich für das nemliche w,

$$6.\quad uv = \mathfrak{G}z + w$$

ist, so kann kein u *oder* v *einem der* x *gleich sein.*

VI. *a. Die Anzahl der Quadratreste, oder die Anzahl der verschiedenen* w *in* (2.) *für alle die zu* z *theilerfremden Zahlen* $> 0 < z$, *ist für kein* z *gröfser als die Hälfte der Zahl der sämmtlichen zu* z *theilerfremden Zahlen* > 0 *und* $< z$.

b. Die Anzahl der Nichtquadratreste, oder die Anzahl der verschiedenen w *in* (1.), *für alle die ungleichen Paare zu* z *theilerfremden Zahlen* $> 0 < z$, *ist für kein* z *kleiner als die Hälfte der Zahl der sämmtlichen zu* z *theilerfremden Zahlen* > 0 *und* $< z$.

Beispiel. Es sei

$$7.\quad z = 15.$$

Die zu z theilerfremden Zahlen sind

$$8.\quad 1, 2, 4, 7, 8, 11, 13 \text{ und } 14;$$

und alle diese Werthe können in (1.) u, v und w haben.

Es sei z. B.

$$9.\quad w = 4 \quad \text{und} \quad w = 11,$$

so ist

$$10.\ \left\{\begin{array}{l} 1.11 = \mathfrak{G}z + 11, \\ 2.13 = \mathfrak{G}z + 11, \\ 4.14 = \mathfrak{G}z + 11, \\ 7.\ 8 = \mathfrak{G}z + 11, \\ 8.\ 7 = \mathfrak{G}z + 11, \\ 11.\ 1 = \mathfrak{G}z + 11, \\ 13.\ 2 = \mathfrak{G}z + 11, \\ 14.\ 4 = \mathfrak{G}z + 11, \end{array}\right. \qquad 11.\ \left\{\begin{array}{l} 1.\ 4 = \mathfrak{G}z + 4, \\ 2.\ 2 = \mathfrak{G}z + 4, \\ 4.\ 1 = \mathfrak{G}z + 4, \\ 7.\ 7 = \mathfrak{G}z + 4, \\ 8.\ 8 = \mathfrak{G}z + 4, \\ 11.14 = \mathfrak{G}z + 4, \\ 13.13 = \mathfrak{G}z + 4, \\ 14.11 = \mathfrak{G}z + 4. \end{array}\right.$$

Zu I. Die *Anzahl* der *Nichtquadrate* oder Producte *ungleicher* Factoren links in (10.) ist 8, in (11.) 4; beides *gerade;* gemäfs (I.).

Zu II. Jedes *Nichtquadrat* kommt in (10. und 11.) *zweimal* vor, und die Hälfte der Zahl der Nichtquadrate 1.11, 2.13, 4.14, 7.8 in (10.) enthält schon *alle* Werthe, welche u und v in (1.) haben können; gemäfs (II.).

Zu III. Die *Anzahl* der Quadrate oder der Producte *gleicher* Factoren links in (10.) ist 0 und in (11.) 4; beides *gerade;* gemäfs (III.).

Zu IV. In (10.) ist z. B. $2^2 = \mathfrak{S}z+4$ und $13^2 = \mathfrak{S}z+4$, und 2.13 ist $= 26 = \mathfrak{S}z-4$. Eben so ist $7^2 = \mathfrak{S}z+4$ und $8^2 = \mathfrak{S}z+4$, und 7.8 ist $= 56 = \mathfrak{S}z-4$; gemäfs (IV.).

Zu V. Keiner der Factoren 1, 4, 11 und 14 der Nichtquadrate in (11.) ist eine Quadratwurzel für z zu w. Diese sind 2, 7, 8 und 13; gemäfs (V.).

Beweis von I. *A.* Wenn man in (1.) u *alle* z_φ durchlaufen läfst, während w *denselben* Werth behält, so durchläuft auch v nach (§. 85. II.) *alle* z_φ. Ist also u_1 irgend ein bestimmter Werth von u, und v_1 der zugehörige, von u_1 verschiedene Werth von v, so dafs auch

$$12.\quad u_1 v_1 = \mathfrak{S}z+w$$

ist, so mufs u, indem es *alle* z_φ durchläuft, aufser diesem Werth u_1 auch nothwendig den Werth v_1 berühren. Zu diesem Werth v_1 von u ist dann auch umgekehrt der *zugehörige* Werth von v offenbar u_1, indem gemäfs (12.) auch

$$13.\quad v_1 u_1 = \mathfrak{S}z+w$$

sein soll. Aber auch keinen andern Werth mehr kann weder v_1 in (12.), noch u_1 in (13.) haben. Denn wäre z. B. in (12. und 13.) noch

$$14.\quad u_1 v_2 = \mathfrak{S}z+w \quad\text{und}\quad 15.\quad v_1 u_2 = \mathfrak{S}z+w,$$

so gäbe (12. und 14.) und (13. und 15.)

$$16.\quad u_1(v_1-v_2) = \mathfrak{S}z \quad\text{und}\quad 17.\quad v_1(u_1-u_2) = \mathfrak{S}z;$$

was Beides nicht sein kann, indem u_1 und v_1 mit z keinen Factor gemein haben und z in v_1-v_2 oder u_1-u_2 allein nicht aufgeht, da $v_1-v_2 < z$ und $u_1-u_2 < z$ ist.

Es können also *dieselben* ungleichen Factoren u_1 und v_1 für das gleiche w *nur zweimal* vorkommen. Aber zweimal kommen sie *nothwendig* vor. Mithin sind die *Nichtquadrate* zu gleichen w immer *paarweise* vorhanden, und daher ist ihre Gesammt-Anzahl *immer gerade;* gemäfs (I.).

Beweis von II. *B. Zwei* ungleiche Factoren u und v_1 kommen nach (*A.*) für ein- und dasselbe w *beide zugleich* je nur noch einmal vor.

Man setze nemlich, ein *einzelner* der beiden Factoren, z. B. u_1, komme noch zum drittenmal vor, verbunden mit einem andern *v*, z. B. v_2. Dann fände (12.) und (14.) Statt, und daraus würde (16.) folgen. Aber (16.) kann, wie dort bemerkt, *nicht* Statt finden. Also kann auch ein einzelner von den beiden Factoren u_1 und v_1 nicht zum drittenmal vorkommen.

Daraus folgt, dafs in zwei *Nichtquadraten,* welche *kein Paar* sind, oder in welchen nicht die *beiden* Factoren dieselben sind, nothwendig *alle vier* Factoren verschieden sein müssen. Und hieraus folgt weiter, dafs schon die *Hälfte* der sämmtlichen Nichtquadrate, nemlich je einer aus jedem Paar genommen, *alle* die z_φ und jedes nur einmal enthalten müssen, welchen *u* und *v* in $uv = \mathfrak{G}z + w$ für ein- und dasselbe *w* überhaupt gleich sein können; gemäfs (II.).

Beweis von III. *C. a.* Wenn

$$18. \quad x^2 = \mathfrak{G}z + w$$

ist, so ist auch, für *dasselbe w,*

$$19. \quad (z-x)^2 = \mathfrak{G}z + w;$$

denn $(z-x)^2$ ist $= z^2 - 2zx + x^2 = \mathfrak{G}z + x^2$, also zufolge (18.) $= \mathfrak{G}z + \mathfrak{G}z + x^2 = \mathfrak{G}z + x^2$.

b. Nun ist ferner $z-x$ immer nothwendig von *x verschieden.* Denn wäre $z-x=x$, so wäre $z=2x$: also müfste *x* in *z aufgehen*, was nicht sein kann, da *x* und *z* nach der Voraussetzung keinen Factor >1 gemein haben. Es kann nur in dem einzigen Falle $z=2x$ sein, wenn $z=2$, also $x=1$ ist. Dieser Fall ist daher, wie in (III.) bemerkt, *ausgenommen.*

c. Da also nun *x* und $z-x$ *verschieden* sind, so gehört nach (*a.*) nothwendig zu jedem Werth, welchen *x* haben kann, ein zweiter, davon *verschiedener* Werth $z-x$. Mithin folgt, dafs die *Quadratwurzeln* für *z* zu *w* immer *paarweise* vorhanden sind und dafs daher ihre Gesammt-Anzahl nothwendig *immer gerade* ist; den einzigen Fall $z=2$ ausgenommen; gemäfs (III.).

Beweis von IV. *D.* Zu jeder Quadratwurzel x_1 für *z* zu *w* gehört nach (*C.*) die zweite $x_2 = z - x$. Nun ist

$$20. \quad x_1 x_2 = x_1(z-x_1) = x_1 z - x_1^2 = \mathfrak{G}z - x_1^2.$$

Aber

$$21. \quad x_1^2 = \mathfrak{G}z + w,$$

also ist, (21. in 20.) gesetzt,

$$22. \quad x_1 x_2 = \mathfrak{G}z - \mathfrak{G}z - w = \mathfrak{G}z - w;$$

gemäfs (IV.).

Beweis von V. *E.* Es sei x eine der *Quadratwurzeln* für z zu w, und u und v seien die ungleichen Factoren eines der *Nichtquadrate* für z zu dem *nemlichen* w, so dafs also

$$23.\quad x^2 = \mathfrak{G}z + w \text{ und}$$

$$24.\quad uv = \mathfrak{G}z + w$$

wäre. Alsdann würde aus (23. und 24.)

$$25.\quad x^2 - uv = \mathfrak{G}z$$

folgen.

Könnte nun x zugleich einer der Factoren u oder v, z. B. $x = u$, sein, so müfste nach (25.)

$$26.\quad x^2 - xv = x(x-v) = \mathfrak{G}z$$

sein und also z in $x(x-v)$ *aufgehen.* Dies aber ist nicht möglich, da x mit z keinen Factor > 1 gemein hat, und $x - v$ *allein* mit z nicht aufgeht, indem es $< z$ ist. Also kann keiner der *Factoren* der *Nichtquadrate* zugleich eine der *Quadratwurzeln* für z zu w sein; gemäfs (V.).

Beweis von VI. *F.* Es sei x irgend eine der zu z theilerfremden Zahlen > 0 und $< z$, so ist auch $z - x$, welches ebenfalls > 0 und $< z$ ist, eine solche Zahl; denn wäre $z - x$ *nicht* zu z theilerfremd, sondern hätte mit z den Stammtheiler $\delta > 1$ gemein, so dafs

$$27.\quad z - x = \mathfrak{G}\delta$$

wäre, so müfste δ, weil es in z aufgeht, nach (§. 18.) auch in x aufgehen, und x und z hätten also den Theiler $\delta > 1$ gemein; gegen die Voraussetzung.

Wenn nun, wie in (2.),

$$28.\quad x^2 = \mathfrak{G}z + w,$$

also w, welches ebenfalls zu den zu z theilerfremden Zahlen > 0 und $< z$ gehört, einer der *Quadratreste* zu z ist, so giebt $z - x$ den *nemlichen* Werth von w; denn es ist

$$29\quad (Z - x)^2 = \mathfrak{G}z + x^2 = \mathfrak{G}z + \mathfrak{G}z + w \ (28.) = \mathfrak{G}z + w.$$

Läfst man nun x in (28. oder 2.) *alle* die zu z theilerfremden Zahlen > 0 und $< z$, deren Anzahl φz bezeichnet, durchlaufen, so kommt nothwendig jeder der *Quadratreste* w *wenigstens zweimal* vor, und folglich kann es für kein z *mehr* als $\frac{1}{2}\varphi z$ *Quadratreste* geben.

Und da nun *nicht mehr* als die *Hälfte* der φz zu z theilerfremden Zahlen > 0 und $< z$ *Quadratreste* sein können, so müssen die übrigen nothwendig *Nichtquadratreste* sein: folglich kann es auch für *kein* z *weniger* als $\frac{1}{2}\varphi z$ *Nichtquadratreste* geben; gemäfs (VI.).

§. 91.

Lehrsatz.

Wenn in der Gleichung

$$1. \quad x^2 = \mathfrak{G}z + 1$$

x *eine zu* z *theilerfremde Zahl* z_φ *bezeichnet, so giebt es*

I. *Was auch* z *sein mag, von* x *immer das Paar ungleicher Werthe*

$$2. \quad x = 1 \quad und \quad x = z - 1.$$

Blofs in dem Falle z = 2 *sind diese Werthe von* x *beide* = 1, *und also nicht ungleich.*

II. *Ist* z *eine Stammzahl, so giebt es für* x *in* (2.) *nur das einzige Werthenpaar* (2.).

III. *Ist* z > 2 *nicht eine Stammzahl, so kann es der Werthe von* x *in* (1.), *so wie überhaupt für*

$$3. \quad x^2 = \mathfrak{G}z + w,$$

wo w *nicht* = 1 *ist, mehrere geben; aber sie sind immer paarweise, also in gerader Zahl vorhanden. Wieviel Werthenpaare von* x *es für* (1.) *oder* (3.) *geben könne, hängt, wie sich weiter unten zeigen wird, von den verschiedenen Factorenpaaren von* z *ab.*

Beispiel zu II. Es sei $z = 7$, so ist $z_\varphi = 1, 2, 3, 4, 5, 6$ und $(1^2, 2^2, 3^2, 4^2, 5^2, 6^2) = \mathfrak{G}z + 1, 4, 2, 2, 4$ und 1. Also *nur* $x = 1$ und $x = z - 1 = 6$ geben $\mathfrak{G}z + 1$.

Zu III. Es sei $z = 15$, so ist $z_\varphi = 1, 2, 4, 7, 8, 11, 13$ und 14 und $(1^2, 2^2, 4^2, 7^2, 8^2, 11^2, 13^2, 14^2) = \mathfrak{G}z + 1, 4, 1, 4, 4, 1, 4, 1, 4, 1$, also $x = 1$ und 14, 4 und 11 geben $\mathfrak{G}z + 1$, so dafs also *zwei* Werthenpaare von x vorhanden sind, welche $x^2 = \mathfrak{G}z + 1$ geben.

Desgleichen geben die *zwei* Werthenpaare 2 und 13 und 7 und 8 $\mathfrak{G}z + 4$ für $w = 4$ in (3.).

Beweis *A.* Was (I.) behauptet ist an sich selbst klar; denn 1^2 und $(z-1)^2$ ist *immer* $= \mathfrak{G}z + 1$; was auch z sei. Ist $z = 2$, so ist $1 = z - 1 = 1$.

B. Gäbe es für eine *Stammzahl* z aufser 1 und $z - 1$ noch ein anderes Werthenpaar x_1 und $z - x_1$, so dafs

$$4. \quad x_1^2 = \mathfrak{G}z + 1 \quad \text{und} \quad (z - x_1)^2 = \mathfrak{G}z + 1$$

wäre, so müfste, da zugleich nothwendig

$$5. \quad 1^2 = \mathfrak{G}z + 1 \quad \text{und} \quad (z-1)^2 = \mathfrak{G}p + 1$$

ist, (5.) von (4.) abgezogen,

$$(x_1^2 - 1) = \mathfrak{G}z \text{ und } (z - x_1)^2 - (z - 1)^2 = \mathfrak{G}z \text{ oder}$$

6. $(x_1 - 1)(x_1 + 1) = \mathfrak{G}z$ und $(z - x_1 - (z - 1))(z - x_1 + z - 1) = \mathfrak{G}z$ oder

$$(1 - x_1)(2z - (x_1 + 1)) = \mathfrak{G}z \text{ sein}$$

und also $(x_1 - 1)(x_1 + 1)$ und $(1 - x_1)(2z - (x_1 + 1))$ mit z *aufgehen.* Eins und das Andere ist nicht der Fall. Denn da x_1 nicht 1 und auch nicht $z - 1$, sondern > 1 und $< z - 1$ sein soll, so geht weder $x_1 - 1$, noch $x_1 + 1$, noch $1 - x_1$, noch $2z - (x_1 + 1)$ mit z auf. Also giebt es, wenn z eine *Stammzahl* ist, für x in (1.) *nur das eine* Werthenpaar 1 und $z - 1$; gemäfs (II.).

C. Ist $z > 2$, und *nicht* eine Stammzahl, so kann es allerdings mit

7. $x_1^2 = \mathfrak{G}z + w$ und $(z - x_1)^2 = \mathfrak{G}z + w$

zugleich, sowohl für $w = 1$, für welchen Fall wenigstens das eine $x_1 = 1$ Statt findet, als für andere Werthe von w, wenn es für solche ein x_1 giebt, auch noch andere Werthe x_2 von x,

8. $x_2^2 = \mathfrak{G}z + w$ und $(z - x_2)^2 = \mathfrak{G}z + w$

geben: denn (8.) von (7.) abgezogen giebt

$$x_1^2 - x_2^2 = \mathfrak{G}z \text{ und } (z - x_1)^2 - (z - x_2)^2 = \mathfrak{G}z \text{ oder}$$

9. $(x_1 - x_2)(x_1 + x_2) = \mathfrak{G}z$ und $(x_2 - x_1)(2z - (x_1 + x_2)) = \mathfrak{G}z$,

und hier können allerdings $x_1 - x_2$ oder $x_2 - x_1$ mit einigen der Factoren von $z > 1$, und $x_1 + x_2$ mit den übrigen Factoren aufgehen. Also kann es in diesem Fall allerdings, sowohl für $w = 1$ in (1.), als für andere Werthe von w in (3.), mehr als ein Werthenpaar von x geben. Auch zeigt sich aus (9.), dafs die Anzahl der möglichen Werthenpaare von x von den verschiedenen Factorenpaaren abhängt, in welche z sich zerlegen läfst; gemäfs (III.).

§. 92.

Lehrsatz.

Man bezeichne die zu einer beliebigen Zahl z > 2 ***theilerfremden*** φz ***Zahlen*** > 0 ***und*** $<$ z ***durch***

1. $z_1, z_2, z_3, z_4, \ldots z_{\varphi z}$,

während jede derselben durch z_φ ***ausgedrückt wird. Ferner sei das Product aller dieser Zahlen***

2. $z_1 z_2 z_3 \ldots z_{\varphi z} = Z$,

und n ***bezeichne die Anzahl der Werthenpaare, welche*** x ***in der Gleichung***

3. $x^2 = \mathfrak{G}z + 1$

haben kann (§. 91. III.), ***unter der Bedingung, dafs*** x ***aus den Zahlen*** z_φ (1.) ***genommen werde.***

I. *Alsdann ist, was auch $z > 2$ sein mag,*

4. $Z = \mathfrak{G}z + 1$, *wenn* n *gerade und*

5. $Z = \mathfrak{G}z - 1$, *wenn* n *ungerade ist.*

Ob n *gerade oder ungerade sei, hängt, wie schon in* (§. 91. III. *und C.*) *bemerkt, von den verschiedenen Factorenpaaren ab, in welche* z *sich zerlegen läſst; wovon weiter unten.*

II. *Für jeden Nichtquadratrest* $w = z_\varphi$ *zu* z, *also für jedes* $w = z_\varphi$, *welches der Gleichung*

$$6. \quad uv = \mathfrak{G}z + w$$

entspricht, wo u *und* v, *eben wie* w, *aus den zu* z *theilerfremden Zahlen* z_φ *genommen, aber nicht einander gleich sind, ist*

$$7. \quad Z = \mathfrak{G}z + w^{\frac{1}{2}\varphi z}.$$

Beispiel zu I. Es sei $z = 15$. Alsdann ist z_φ (1.) $= 1, 2, 4, 7, 8, 11, 13$ und 14, und das Product dieser z_φ ist $Z = 1.2.4.7.8.11.13.14 = 896\,896 = 59793.z + 1$, während die Zahl n der Werthenpaare 1 und 14 und 4, 11 von x in (3.), welche $x^2 = \mathfrak{G}z + 1$ geben, $= 2$, also *gerade* ist; gemäſs (4.).

Es sei $z = 18$. Alsdann ist z_φ (1.) $= 1, 5, 7, 11, 13$ und 17, und das Product dieser z_φ ist $Z = 1.5.7.11.13.17 = 85085 = 4727.z - 1$. Hier giebt nur das *eine* Werthenpaar 1 und 17 von x in (3.) $\mathfrak{G}z + 1$, so daſs $n = 1$ und also *ungerade* ist; gemäſs (5.).

Beispiel zu II. Einer der *Nichtquadratreste* zu $z = 15$ ist $w = 11$, und $\frac{1}{2}\varphi z$ ist $= 4$; desgleichen ist $Z = 1.2.4.7.8.11.13.14 = 896\,896$. Also soll nach (7.) $896\,896 = \mathfrak{G}.15 + 11^4 = \mathfrak{G}15 + 14641$ sein, und in der That ist

$$896\,896 = 18817.15 + 14641.$$

Beweis von I. *A.* Wenn man in der Gleichung

$$8. \quad uv = \mathfrak{G}z + w,$$

wo w jede der Zahlen z_φ (1.) sein kann, u alle z_φ durchlaufen läſst, so durchläuft nach (§. 85. II.), für *ein- und dasselbe w,* auch v alle die Zahlen z_φ; wiewohl in verschiedener Ordnung.

B. Nun kann nach (§. 90.) u und v sowohl *ungleich* als *gleich* sein; d. h. es kann w sowohl *Nichtquadratrest* als *Quadratrest* sein. Für den letztern Fall schreibe man, wie in (§. 90.), x statt der *gleichen u* und *v.*

C. Nach (§. 90. I. und III.) sind aber sowohl die *Nichtquadrate uv,* als die *Quadrate* x^2, für ein- und dasselbe w immer *paarweise* vorhanden, und die Gesammtzahl der *Nichtquadrate,* so wie der *Quadrate,* ist immer

gerade. Jene, die Anzahl der ***Nichtquadratenpaare,*** werde durch m, die der ***Quadratenpaare,*** wie hier oben für den Rest $w = 1$, allgemein für ***jedes*** w durch n bezeichnet.

D. Läſst man also nun u in (8.) alle z_φ durchlaufen und bezeichnet die zusammengehörigen u und v durch $u_1, v_1; u_2, v_2; u_3, v_3; \ldots u_{\varphi z}, v_{\varphi z}$, so daſs

$$9. \begin{cases} u_1 v_1 = \mathfrak{G} z + w, \\ u_2 v_2 = \mathfrak{G} z + w, \\ u_3 v_3 = \mathfrak{G} z + w, \\ \ldots\ldots\ldots\ldots \\ u_{\varphi z} v_{\varphi z} = \mathfrak{G} z + w \end{cases}$$

ist, wo nun die v nach (§. 85. II.) ebenfalls, gleich den u, *alle* z_φ sind, so befinden sich unter den φz Gleichungen (9.) $2m$ Gleichungen, in welchen u und v *nicht* einander gleich sind, und $2n$ Gleichungen, in welchen $u = v = x$ ist.

E. Demnach zerfallen also die φz Gleichungen (7.) in folgende ***zwei verschiedene Gruppen:***

$$10. \begin{cases} u_1 v_1 = \mathfrak{G} z + w, \\ u_2 v_2 = \mathfrak{G} z + w, \\ u_3 v_3 = \mathfrak{G} z + w, \\ \ldots\ldots\ldots \\ u_{2m} v_{2m} = \mathfrak{G} z + w \end{cases} \quad \text{und} \quad 11. \begin{cases} x_1^2 = \mathfrak{G} z + w, \\ x_2^2 = \mathfrak{G} z + w, \\ x_3^2 = \mathfrak{G} z + w, \\ \ldots\ldots\ldots \\ x_{2n}^2 = \mathfrak{G} z + w. \end{cases}$$

F. Nach (§. 90. II.) enthält schon die ***Hälfte*** der ***Nichtquadratreste*** uv in (10.) ***alle*** Werthe, welche u und v haben können; und nach (§. 90. V.) kann kein u oder v in (8.) einem x in (11.) ***gleich*** sein, so daſs also die x in (11.) durchaus ***andere*** z_φ sind, als die u und v in (10.), während (10. und 11.) zusammen nothwendig ***alle*** z_φ enthalten; wie die Gleichungen (9.), aus welchen sie entnommen sind. Endlich gehört nach (§. 90. IV.) zu jedem x in (11.) ein zweites $z - x$, welches, mit ihm multiplicirt, $\mathfrak{G} z - w$ giebt.

G. Nimmt man also aus den Gleichungen (10.) diejenige ***Hälfte*** m heraus, welche ***sämmtlich verschiedene*** u und v oder z_φ enthalten; desgleichen die ***sämmtlichen*** Gleichungen (VI.), welche n ***verschiedene Werthenpaare*** x und $z - x$ von x und sämmtlich ***andere*** z_φ enthalten, so kommen nothwendig in diesen $m + 2n$ Gleichungen zusammen ***alle*** z_φ vor; und alle ***nur einmal.***

H. Multiplicirt man also jene aus (10.) genommenen m Gleichungen, mit sämmtlich verschiedenen z_φ, in einander und mit den $2n$ Gleichungen (11.), so hat man ***links*** das Product ***aller*** z_φ und jedes z_φ, in denselben ***nur einmal,*** also das Product $\mathbf{Z}$ (2.). ***Rechts*** geben zunächst die m Gleichungen aus (10.)

$(\mathfrak{S}z+w)^m$. Sodann geben die $2n$ Gleichungen (11.), weil *jedes der n Paare zusammengehöriger* x, nemlich x und $z-x$, nach (§. 90. IV.), $\mathfrak{S}z-w$ giebt, $(\mathfrak{S}z-w)^n$. Also ist das Product *aller* der $m+2n$ Gleichungen

$$12. \quad Z = (\mathfrak{S}z+w)^m(\mathfrak{S}z-w)^n.$$

I. Dieses Ergebnifs gilt für *jeden* Werth, welchen w haben kann. Es kann aber w jedenfalls $=1$ für jedes z sein (§. 91.). Also gilt (12.) auch für $w=1$ und giebt alsdann

$$13. \quad Z=(\mathfrak{S}z+1)^m(\mathfrak{S}z-1)^n=(\mathfrak{S}z+1)(\mathfrak{S}z+(-1)^n)=\mathfrak{S}z+(-1)^n,$$

und folglich ist

$$14. \quad Z=\mathfrak{S}z+1, \text{ wenn } n \text{ gerade ist; gemäfs (4.), und}$$

$$15. \quad Z=\mathfrak{S}z-1, \text{ wenn } n \text{ ungerade ist; gemäfs (5.).}$$

K. *Wenn* n gerade oder ungerade sei, darauf wird zunächst weiter der Lehrsatz (§. 94.) führen.

Beweis von II. *L.* Für die Gleichung

$$16. \quad uv = \mathfrak{S}z+w$$

kommen nach (§. 90. II.) schon in der *Hälfte der Nichtquadrate uv* für ein- und denselben Nichtquadratrest w alle die φz Werthe von z_φ vor, welche u und v haben können, und jeder dieser Werthe nur einmal.

Also schon die *Hälfte* der φz Producte uv in (16.) enthält alle z_φ, und jedes nur einmal. Mithin erhält man, wenn man diese *Hälfte* der φz Producte uv in (16.) in einander multiplicirt, die Gröfse $z_1 z_2 z_3 \ldots z_{\varphi z} = Z$ (2.); und da nun *jedes* dieser $\frac{1}{2}\varphi z$ Producte durch $\mathfrak{S}z+w$ ausgedrückt wird (16.), so ist

$$17. \quad Z = (\mathfrak{S}z+w)^{\frac{1}{2}\varphi z} = \mathfrak{S}z+w^{\frac{1}{2}\varphi z};$$

gemäfs (7.).

§. 93.

Fünfter Beweis des Wilsonschen Lehrsatzes (§. 48.).

A. Wenn z eine *Stammzahl* ist, so ist

$$1. \quad z_\varphi = 1, 2, 3, 4, \ldots z-1,$$

also in (§. 92. 2.)

$$2. \quad Z = 1.2.3.4 \ldots z-1.$$

B. Nun giebt es nach (§. 91. II.), wenn z eine *Stammzahl* ist, *nur* das *einzige* Werthenpaar 1 und $z-1$ von x, für welches in (§. 92. 3.) $x^2=\mathfrak{S}z+1$ ist. Also ist dann n in (§. 92.) $=1$, und folglich *ungerade.* Mithin ist alsdann nach (§. 92. 5.) $Z=Nz-1$ und folglich in (2.)

$$3. \quad 1.2.3.4 \ldots z-1 = \mathfrak{S}z-1.$$

Dieses ist der *Wilson*sche Lehrsatz (§. 48.).

§. 94.

Lehrsatz.

Wenn z *eine beliebige Zahl ist und* x *beliebige, aus den* φz *zu* z *theilerfremden Zahlen* > 0 *und* $< z$ *bezeichnet, so sind nach* (§. 90. III. *und* IV.) *die Werthe von* x, *die der Gleichung*

$$1. \quad x^2 = \mathfrak{G}z + r$$

genugthun, in welcher r *nach* (§. 85.) *nothwendig stets ebenfalls eine der zu* z *theilerfremden Zahlen* z_φ *ist, immer paarweise vorhanden; und zwar, wenn* x_1 *der eine Werth von* x *ist, so ist* $z - x_1$ *der andere.*

Für $r = 1$ *in* (1.), *also für die Gleichung*

$$2. \quad x^2 = \mathfrak{G}z + 1,$$

haben wir in (§. 92.) *die Anzahl der Werthenpaare von* x, *die diese Gleichung erfüllen, durch* n *bezeichnet, so dafs also, wenn man* x *in der Gleichung* (1.) *alle* z_φ *durchlaufen läfst,* 2n *dieser Werthe* z_φ *von* x *in* (2.) *den Rest* $r = 1$ *geben.*

Ferner haben wir in (§. 92.) *und auch schon in* (§. 91. III.) *bemerkt, dafs jene Zahl* n *von der Anzahl und Art der Factorenpaare abhängt, in welche* z *sich zerlegen läfst.*

Mit der Anzahl n *der Quadratwurzelpaare, für einen und denselben Rest* r, *ferner mit der Anzahl der möglichen verschiedenen Quadratreste* r *selbst in* (1.) *für ein bestimmtes* z, *und mit den Eigenschaften dieser Quadratreste* r *verhält es sich nun weiter wie folgt.*

I. *Zu andern Werthen von* r *in* (1.) *gehören andere* x; *also, wenn man die zu einem bestimmten* r *gehörigen* x *durch* x_r *und die zu einem andern* r_1 *gehörigen* x *durch* x_{r_1} *bezeichnet, so kann nicht* $x_r = x_{r_1}$ *sein.*

II. *Zu jedem Werth, welchen* r *in* (1.) *haben kann, gehören gleich viele* x; *also gehören, da immer* $r = 1$ *sein kann, und folglich die Gleichung* (2.) *mit ihren* 2n *verschiedenen Werthen von* x *immer Statt findet, zu jedem* r *in* (1.) 2n *verschiedene und zu jedem* r, 2n *andere* x. *Man findet diese* 2n *andern Werthe von* x_r *für ein bestimmtes* r, *z. B. aus den* 2n *Werthen von* x_1 *für* $r = 1$ *in* (2.), *wenn man in der Gleichung*

$$3. \quad x_1 x_r = \mathfrak{G}z + (x_r)$$

dem x_r *links irgend einen der Werthe von* x_r, *gleichviel welchen, dem andern Factor* x_1 *aber der Reihe nach alle die* 2n *Werthe beilegt, welche*

x_1 *in* (2.) *haben kann. Alsdann drückt* (x_r) *rechts alle die Werthe aus, welche* x_r *haben kann; und sie alle thun der Gleichung* (1.) *Genüge.*

III. *Die verschiedenen* x, *zu den verschiedenen* r *gehörig, sind alle die* φz *zu* z *theilerfremden Zahlen* $z_\varphi > 0$ *und* $< z$, *und jede kommt, wenn man* r *seine verschiedenen Werthe durchlaufen läfst, nur einmal vor; so also, dafs, wenn man die Anzahl der zu* z *Statt findenden verschiedenen Quadratreste* r *durch* ν *bezeichnet,*

$$4. \quad \varphi z = 2n\nu$$

ist.

IV. *Das Product einer beliebigen Anzahl gleicher oder ungleicher Quadratreste* r, *also auch eine beliebige Potenz eines Quadratrestes* r, *läfst, durch* z *dividirt, immer wieder einen der Quadratreste zum Rest, so dafs also immer*

$$5. \begin{cases} 1. \quad r_1 r_2 r_3 \ldots r_\sigma = \mathfrak{G}z + r_\mu \text{ und} \\ 2. \quad r^\tau = \mathfrak{G}z + r_\mu \end{cases}$$

ist, wo r_μ *irgend eines der* r *bezeichnet und* σ *in* (5. 1.) *und* τ *in* (5. 2.) *beliebige positive ganze Zahlen sein können.*

V. *Für jeden der Quadratreste* r *ist*

$$6. \quad r^\nu = \mathfrak{G}z + 1,$$

oder, nach (4.) *ausgedrückt,*

$$7. \quad r^{\frac{\varphi z}{2n}} = \mathfrak{G}z + 1;$$

doch können auch schon niedrigere Potenzen von r *als die* ν*te, durch* z *dividirt, den Rest* 1 *lassen. Jedenfalls aber giebt die* ν*te Potenz von* r *den Rest* 1.

VI. *Wenn man*

$$8. \quad x_1^2 = \mathfrak{G}z + 1 \text{ und } x_r^2 = \mathfrak{G}z + r,$$

und dann weiter

$$9. \quad r^2 = \mathfrak{G}z + \overset{1}{r},$$

$$10. \quad r x_1 = \mathfrak{G}z + (\overset{1}{x})$$

setzt, so ist ($\overset{1}{x}$) *in* (10.) *ebenfalls eines der zu* $\overset{1}{r}$ *in* (9.) *gehörigen* x, *also*

$$11. \quad (\overset{1}{x})^2 = \mathfrak{G}z + \overset{1}{r},$$

und für jedes r *in* (9.) *und* (10.) *ein anderes. Man findet also auch zu* $r > 1$ *gehörige* x *aus denen, welche zu* $r = 1$ *gehören, wenn man die letzteren nach* (10.) *mit* r *multiplicirt und das Product durch* z *dividirt.*

VII. *Geht* z *mit* 2 *auf, so geben nicht blofs* x *und* z—x, *wie für jedes beliebige* z, *sondern auch*

$$12.\quad x,\ \tfrac{1}{2}z - x,\ \tfrac{1}{2}z + x \text{ und } z - x$$

einen und denselben Quadratrest r *zu* z.

VIII. *Da nach* (II.) *zu jedem Werth, welchen* r *haben kann, gleichviele* x *gehören, so kommt es nur darauf an, wie viele verschiedenen Werthe* x *es für die Gleichung*

$$13.\quad x^2 = \mathfrak{G}z + 1\ (2.)$$

giebt. Ebensoviele Werthe hat x *in der Gleichung* (1.) *für jedes* r.

Die Anzahl der verschiedenen in (13.) *möglichen* x *nun läfst sich finden, wenn man* z *auf alle mögliche Weise in zwei Factoren* $\varkappa$ *und* λ *zerlegt, also*

$$14.\quad z = \varkappa\lambda$$

und statt (13.) $x^2 = \mathfrak{G}\varkappa\lambda + 1$ *setzt, woraus* $x^2 - 1 = \mathfrak{G}\varkappa\lambda$ *oder*

$$15.\quad (x+1)(x-1) = \mathfrak{G}\varkappa\lambda$$

folgt. Man kann dann die Bedingung machen, dafs x+1 *mit dem einen der Factoren* $\varkappa = \lambda$, x—1 *mit dem andern aufgehe. Alsdann verhält es sich mit den verschiedenen* x, *die der Gleichung* (13.) *genugthun, wie folgt.*

a. Für Factorenpaare $\varkappa$ *und* λ *von* z, *welche einen gröfsern Gemeintheiler als* 2 *haben, giebt es kein* x *für* (13.).

b. Zu jedem theilerfremden Paare von Factoren $\varkappa$ *und* λ *von* z, *die beide ungerade sind, gehört ein, und nur ein Werthenpaar von* x, *nemlich*

$$16.\quad \overset{1}{x} = x \text{ und } \overset{2}{x} = z - x,$$

und jedes andere Factorenpaar dieser Art giebt ein anderes Werthenpaar von x.

c. Zu jedem theilerfremden Paare von Factoren $\varkappa$ *und* λ *von* z, *deren einer ungerade ist, während der andere mit* 2, *aber nur mit der ersten Potenz von* 2 *aufgeht, gehört ebenfalls ein, und nur ein Werthenpaar von* x, *wie das* (16.); *aber nicht zu jedem andern Factorenpaare dieser Art gehört ein anderes Werthenpaar von* x, *sondern* $\tfrac{1}{2}\varkappa$ *und* 2λ *oder* $2\varkappa$ *und* $\tfrac{1}{2}\lambda$, *je nachdem* $\varkappa$ *oder* λ *gerade ist, geben das nemliche Werthenpaar von* x, *wie* $\varkappa$ *und* λ *selbst. Und dann kommt von den Werthenpaaren von* x, *die alle den verschiedenen Factorenpaaren dieser Art entsprechen, jedes zweimal vor.*

d. Zu jedem theilerfremden Paare von Factoren $\varkappa$ und λ von z, *deren einer ungerade ist, während der andere mit einer höhern Potenz von* 2 *als der ersten aufgeht, gehört wiederum ein, und nur ein Werthenpaar von* x, *wie das* (16.). *Hier gehört zu jedem andern Factorenpaare dieser Art ein anderes Werthenpaar von* x. *Zwar giebt es je noch ein zweites Factorenpaar von* z, *nemlich* $\frac{1}{2}\varkappa$ *und* 2λ *wenn* λ, *und* $2\varkappa$ *und* $\frac{1}{2}\lambda$ *wenn* $\varkappa$ *ungerade ist, dem das nemliche Werthenpaar von* x *zukommt, wie dem Factorenpaare* $\varkappa$ *und* λ *selbst, aber dieses zweite Factorenpaar findet sich nicht unter denen der gegenwärtigen Art, sondern nur unter denen, die mit* 2 *gemeintheilbar sind.*

e. Zu jedem Paare von Factoren $\varkappa$ *und* λ *von* z, *die beide mit der ersten Potenz von* 2 *aufgehen, gehören zwei, und nur zwei Werthenpaare von* x, *nemlich folgende:*

$$17. \quad \overset{1}{x} = x \quad \textit{und} \quad \overset{2}{x} = z - x,$$

$$18. \quad \overset{3}{x} = \tfrac{1}{2}z + x \quad \textit{und} \quad \overset{4}{x} = \tfrac{1}{2}z - x.$$

Zu jedem andern Factorenpaare der gegenwärtigen Art gehören zwei andere Werthe von x, *wie* (17. *und* 18.). *Zugleich sind zwei von den vier Werthen von* x (17. *und* 18.) *die nemlichen, welche zu dem Factorenpaare* $\frac{1}{2}\varkappa$ *und* 2λ *gehören, wenn* $\frac{1}{2}\varkappa$ *ungerade ist, und zu dem Factorenpaare* $2\varkappa$ *und* $\frac{1}{2}\lambda$, *wenn* $\frac{1}{2}\lambda$ *ungerade ist; und immer ist entweder* $\frac{1}{2}\varkappa$ *oder* $\frac{1}{2}\lambda$ *ungerade.*

IX. *a. Ist* z *ungerade, so geben die theilerfremden Paare von Factoren* (VIII. *b.*), *welche beide ungerade sind, alle* x, *welche der Gleichung* $x^2 = \mathfrak{G}z + 1$ *genugthun. Also giebt es dann eben so viele Werthenpaare von* x, *als theilerfremde Factorenpaare von* z.

b. Geht z *nur mit der ersten Potenz von* 2 *auf, so giebt schon die Hälfte der theilerfremden Paare von Factoren* (VIII. *c.*), *deren einer gerade, der andere ungerade ist, alle* x, *welche der Gleichung* $x^2 = \mathfrak{G}z + 1$ *genugthun. Also giebt es in diesem Falle halb so viele Werthenpaare von* x, *als theilerfremde Factorenpaare von* z.

c. Geht endlich z *mit einer höhern als der ersten Potenz von* 2 *auf, so geben schon die verschiedenen mit* 2, *aber mit keiner gröfsern Zahl, gemeintheilbaren Paare von Factoren von* z *allein alle* x, *welche der Gleichung* $x^2 = \mathfrak{G}z + 1$ *genugthun. Also giebt es in diesem Fall*

doppelt so viele Werthenpaare von x, *als durch* 2 *aber durch keine gröfsere Zahl gemeintheilbare Factorenpaare von* z.

Auf solche Weise hängt denn also in Folge der Gesetze (VIII. *und* IX.) *die Anzahl* 2n *der verschiedenen möglichen Quadratwurzeln* x *für* z *zu dem Rest* 1 *in* (13.), *so wie zu jedem beliebigen andern Rest* r, *da jeder beliebige Rest nach* (II.) *immer dieselbe Anzahl* 2n *von* x *zukommt, von der Zahl und Art der Factorenpaare* $\varkappa$ *und* λ *von* z (4.) *ab, aus welchen sich* z *durch die Multiplication zusammensetzen läfst.*

Erstes Beispiel. Es sei

19. $z = 180 = 2^2 . 3^2 . 5.$

Die zu z *theilerfremden* Zahlen $z_\varphi > 0$ und $< z$ sind folgende:

20. $z_\varphi =$ 1 7 11 13 17 19 23 29 31 37 41 43 47 49 53 59 61 67 71 73 77 79 83 89
91 97 101 103 107 109 113 119 121 127 131 133 137 139 143 149 151 157 161 163 167 169 173 179.

Ihre *Anzahl* ist

21. $\varphi z = 48.$

Läfst man nun in (1.) x *alle* diese Zahlen durchlaufen, so findet sich

22.

Für $x =$	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59	61	67	71	73	77	79	83	89
$r =$	1	49	121	169	109	1	169	121	61	109	61	49	49	61	109	61	121	169	1	109	169	121	49	1
Für $x =$	91	97	101	103	107	109	113	119	121	127	131	133	137	139	143	149	151	157	161	163	167	169	173	179,
$r =$	1	49	121	169	109	1	169	121	61	109	61	49	49	61	109	61	121	169	1	109	169	121	49	1.

Es giebt also hier, wie sich zeigt, die

23. $\nu = 6$ verschiedenen *Quadratreste* $r = 1, 49, 61, 109, 121$ und 169, sämmtlich aus den Zahlen z_φ (20.), und zu *jedem* derselben gehören

24. $2n = 8$, also $n = 4$

verschiedene Werthenpaare von x, nemlich

25.
1. zu $r = 1$ gehören die 4 Werthenpaare 1 u. 179, 19 u. 161, 71 u. 109, 89 u. 91 von $x = x_1$,
2. zu $r = 49$ - - - - - - - 7 u. 173, 43 u. 137, 47 u. 133, 83 u. 97 von $x = x_{49}$,
3. zu $r = 61$ - - - - - - - 31 u. 149, 41 u. 139, 49 u. 131, 59 u. 121 von $x = x_{61}$,
4. zu $r = 109$ - - - - - - - 17 u. 163, 37 u. 143, 53 u. 127, 73 u. 107 von $x = x_{109}$,
5. zu $r = 121$ - - - - - - - 11 u. 169, 29 u. 151, 61 u. 119, 79 u. 101 von $x = x_{121}$,
6. zu $r = 169$ - - - - - - - 13 u. 167, 23 u. 157, 67 u. 113, 77 u. 103 von $x = x_{169}$;

sämmtlich in der Form x und $z - x$ begriffen.

Die verschiedenen Behauptungen des Lehrsatzes zeigen sich an diesen Beispielen wie folgt.

I. Zu jedem *andern* Werth von r gehören gemäfs (25.) *andere* x; gemäfs (I.).

II. Zu *jedem* der $\nu = 6$ (23.) verschiedenen r gehören gemäfs (25.) *gleichviele* x, nemlich zu jedem $2n = 8$ verschiedene x; gemäfs (II.).

Man findet ferner, z. B. aus den $2n = 8$ Werthen (25. 1.) von x_1, welche zu $r = 1$ gehören, die zu $r = 61$ gehörigen $2n = 8$ Werthe von $x_r = x_{61}$ (25. 3.), wenn man in der Gleichung (3.) dem x_r links *irgend einen* der Werthe von x_r giebt, z. B. wenn man $x_r = 41$ (25. 3.) setzt, und dann x_1 in (3.) alle seine 8 Werthe 1, 19, 71, 89, 91, 109, 161 und 179 (25. 1.) durchlaufen läfst. Es ergiebt sich auf diese Weise nach (3.)

26. $41(1, 19, 71, 89, 91, 109, 161, 179)$
$= \mathfrak{S}.180 + 41, 59, 31, 49, 131, 149, 121$ und 139,

also ist in (3.)

27. $(x_r) = 41, 59, 31, 49, 131, 149, 121$ und 139;

und dies sind in der That alle die $2n = 8$ Werthe (25. 3.) von $x_r = x_{61}$.

III. Die verschiedenen x zu den verschiedenen r sind gemäfs (25.) *alle* die Zahlen z_φ (20.), und keine derselben kommt mehr als einmal vor, so dafs nach (3.) φz oder 48 (21.) $= 2n.\nu = 8.6$ ist; gemäfs (III.).

IV. Multiplicirt man z. B. die vier Quadratreste 49, 49, 109 und 121 mit einander, so ist das Product $31666789 = 175926.z + 109$, und der Rest 109 ist ebenfalls einer der Quadratreste r (23.). Nimmt man z. B. die 5te *Potenz* des Quadratrestes $r = 61$, so giebt dieselbe $844596301 = 4693201.z + 121$ und der Rest 121 ist wiederum einer der Quadratreste r (23.); gemäfs (IV.).

V. Da hier $\nu = 6$ ist (23.), so soll nach (6.), z. B. für den Quadratrest $r = 49$, $49^6 = \mathfrak{S}z + 1$ sein, und es ist $49^2 = 2401 = \mathfrak{S}z + 61$, also $49^6 = \mathfrak{S}z + 61^3 = \mathfrak{S}z + 226981 = \mathfrak{S}z + 1$; wie es sein soll. Von $r = 61$ ist aber schon die 3te Potenz, und von $r = 109$ schon die 2te Potenz $= \mathfrak{S}z + 1$: also von $r = 61$ und 109 geben auch schon *niedrigere* als die $\nu = 6$te Potenz $\mathfrak{S}z + 1$; gemäfs (V.).

VI. Multiplicirt man z. B. das zu $x_1^2 = \mathfrak{S}z + 1$ gehörige $x_1 = 71$ (25. 1.) der Reihe nach mit $r = 1, 49, 61, 109, 121$ und 169, so giebt (10.)

28. $rx_1 = 71, 3479, 4331, 7739, 8591$ und 11999
$= \mathfrak{S}z + 71, 59, 11, 179, 131$ und 119,

also in (10.)

29. $(x) = 71, 59, 11, 179, 131$ und 119.

Desgleichen giebt (9.) für die nemlichen Werthe von r:

30. $r^2 = 5041, 2401, 3721, 11881, 14641$ und $28561 = \mathfrak{S}z + 1, 61, 121, 1, 61$ und 121,

also in (9.)

$$31.\quad \overset{1}{r} = 1, 61, 121, 1, 61 \text{ und } 121.$$

Es soll also nach (11.)

$$32.\quad 71^2 = \mathfrak{G}z + 1,\ 59^2 = \mathfrak{G}z + 61,\ 11^2 = \mathfrak{G}z + 121,\ 179^2 = \mathfrak{G}z + 1,$$
$$131^2 = \mathfrak{G}z + 61 \text{ und } 119^2 = \mathfrak{G}z + 121$$

sein, was auch, wie aus (22.) zu sehen, in der That der Fall ist; gemäfs (VI.).

VII. Für $x = 41$ ist in $x^2 = \mathfrak{G}z + r$ (1.) gemäfs (22.) $r = 61$, und für $\frac{1}{2}z - x = 90 - 41 = 59$, $\frac{1}{2}z + x = 90 + 41 = 131$ und $z - x = 180 - 41 = 139$ ist r ebenfalls $= 61$; wie es gemäfs (VII. 12.) sein mufs, da $z = 180$ mit 2 aufgeht.

VIII. Die Factorenpaare $\varkappa$ und λ, in welche $z = 180$ sich zerlegen läfst, sind folgende:

33.

$\varkappa =$	1	2	3	4	5	6	9	10	12	15	18	20	30	36	45	60	90	180,
$\lambda =$	180	90	60	45	36	30	20	18	15	12	10	9	6	5	4	3	2	1.

a. Setzt man nun in (15.) z. B. $\varkappa = 12$, $\lambda = 15$, welches Factorenpaar den Theiler $3 > 2$ gemein hat, so geht für *keinen einzigen* der Werthe z_φ (20.), welche x haben könnte, $x + 1$ mit einem der Factoren $\varkappa = 12$ und $\lambda = 15$ und $x - 1$ mit dem andern auf. Legt man nemlich dem x die *erste Hälfte* der Werthe von z_φ (22.) bei (und nur diese ist zu untersuchen, indem, falls in der zweiten Hälfte sich ein passendes x fände, das nothwendig zugehörige $z - x$ in die erste Hälfte fallen würde), so findet sich

34.

Für $x =$	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59	61	67	71	73	77	79	83	89,
$x + 1 =$	2	8	12	14	18	20	24	30	32	38	42	44	48	50	54	60	62	68	72	74	78	80	84	90,
$x - 1 =$	0	6	10	12	16	18	22	28	30	36	40	42	46	48	52	58	60	66	70	72	76	78	82	88;

und von allen diesen $x + 1$ und $x - 1$ geht kein einziges Paar mit 12 und 15 auf. Geht ja $x + 1$ mit 12 oder 15 auf, so geht $x - 1$ nicht mit 15 oder 12 auf. Also giebt es für $\varkappa = 12$ und $\lambda = 15$, deren Gemeintheiler $3 > 2$ ist, *kein x;* gemäfs (VIII. *a.*).

Es müssen demnach in (33.) die Factorenpaare 3 und 60, 6 und 30, 12 und 15, 15 und 12, 30 und 6, 60 und 3 ganz *ausgeschlossen* werden. Von den übrig bleibenden aber ist wiederum nur die *Hälfte* zu berücksichtigen, da sie, blofs *verwechselt,* paarweise *dieselben* sind, und $\varkappa$ oder λ sowohl den einen als den andern Factor von z bezeichnen kann. Es bleiben also nur folgende Factorenpaare von z zu berücksichtigen:

35.

$\varkappa =$	1	2	4	5	9	10,
$\lambda =$	180	90	45	36	20	18.

b. Nimmt man nun von diesen $\varkappa$ und λ, z. B. das *theilerfremde* Factorenpaar 5 und 36, so soll nach (15.)

$$36. \quad (x+1)(x-1) = \mathfrak{G}.5.36$$

sein und $x+1$ mit 5 oder 36 und zugleich $x-1$ mit 36 oder 5 *aufgehen*. Wie aus (34.) zu sehen, erfüllt *nur allein* $x=71$ diese Bedingung. Es giebt also zu dem *theilerfremden* Factorenpaare 5 und 36 von z nur das *einzige* Werthenpaar $x=71$ und $z-x=109$ von x; gemäfs (VIII. *b.*).

Die übrigen theilerfremden Factorenpaare in (35.) sind 1 und 180, 4 und 45, 9 und 20. Zufolge (34.) pafst 1 und 180 nur für $x=1$, 4 und 45 nur für $x=89$, und 9 und 20 nur für $x=19$, also ist zusammen

$$37. \quad \begin{cases} \overset{1}{x} = 71, & \overset{2}{x} = 109 \text{ für } \varkappa, \lambda = 5, \ 36, \\ \overset{1}{x} = 1, & \overset{2}{x} = 179 \text{ für } \varkappa, \lambda = 1, 180, \\ \overset{1}{x} = 89, & \overset{2}{x} = 91 \text{ für } \varkappa, \lambda = 4, \ 45, \\ \overset{1}{x} = 19, & \overset{2}{x} = 161 \text{ für } \varkappa, \lambda = 9, \ 20. \end{cases}$$

Alle diese Werthe von x sind von einander *verschieden;* gemäfs (VIII. *b.*).

c. Eins der Factorenpaare $\varkappa$ und λ von z in (35.), welches 2 zum Gemeintheiler hat, ist 10 und 18. Für dieses also soll in (34.)

$$38. \quad (x+1)(x-1) = \mathfrak{G}.10.18$$

sein und $x+1$ mit 10 oder 18 und zugleich $x-1$ mit 18 oder 10 aufgehen. Zufolge (34.) wird diese Bedingung nur durch $x=19$ und 71 erfüllt, wozu $z-x=161$ und 109 gehört. Ein anderes Factorenpaar $\varkappa$ und λ, mit dem Gemeintheiler 2, ist 2 und 90; und für dieses pafst in (34.) $x=1$ und 89, wozu $z-x=179$ und 91 gehört. Es ist also zusammen, nach der Bezeichnung (17. und 18.),

$$39. \quad \begin{cases} \overset{1}{x}=19, \ \overset{2}{x}=71, \ \overset{3}{x}=109 \text{ und } \overset{4}{x}=161 \text{ für } \varkappa, \lambda = 10, 18 \text{ und} \\ \overset{1}{x}=\ 1, \ \overset{2}{x}=89, \ \overset{3}{x}=\ 91 \text{ und } \overset{4}{x}=179 \text{ für } \varkappa, \lambda = \ 2, 90, \end{cases}$$

und man sieht, dafs gemäfs (17. und 18.) $\overset{2}{x}=\tfrac{1}{2}z-\overset{1}{x}$, $\overset{3}{x}=\tfrac{1}{2}z+\overset{1}{x}$ und $\overset{4}{x}=z-\overset{1}{x}$ ist. Jedes der Factorenpaare mit dem Gemeintheiler 2 giebt also *zwei* Werthenpaare von x; wie es nach (VIII. *c.*) sein soll.

d. Eines der theilerfremden Factorenpaare $\varkappa$ und λ von z in (35.), *von der Art*, wie sie (VIII. *d.*) verlangt, nemlich, dafs einer der Factoren mit einer höhern als der zweiten Potenz von 2 aufgehe, der andere mit 2

gar nicht, ist 4 und 45. Das zu diesem Factorenpaar gehörige eine Werthenpaar von x ist, nach (VIII. *e.*) bezeichnet,

$$40. \quad \overset{1}{(x)} = 89 \text{ und } \overset{2}{(x)} = 91.$$

Ferner ist, wenn man $\varkappa = 4$ und $\lambda = 45$ sein läfst, $\frac{1}{2}\varkappa = 2$ und $2\lambda = 90$. Zu diesem Factorenpaar 2 und 90 gehört nach (39.)

$$41. \quad \overset{1}{x} = 1, \quad \overset{2}{x} = 89, \quad \overset{3}{x} = 91 \text{ und } \overset{4}{x} = 179,$$

und, wie aus (39. und 40.) zu sehen, ist

$$42. \quad \overset{1}{(x)} = \overset{2}{x} \text{ und } \overset{2}{(x)} = \overset{3}{x};$$

gemäfs (VIII. *d.*).

e. Die zu den *theilerfremden* Factoren $\varkappa = 4$ und $\lambda = 45$ gehörigen x sind unter den zu $\frac{1}{2}\varkappa = 2$ und $2\lambda = 90$ gehörigen x mitbegriffen. Auf dieselbe Weise sind, wie aus (37. und 38.) zu sehen, die zu den übrigen theilerfremden Factorenpaaren 5 und 36, 1 und 180 und 9 und 20 gehörigen x, der Reihe nach unter den zu 10 und 18, 2 und 90 und 18 und 10 gehörigen (34.) mitbegriffen; gemäfs (VIII. *e.*).

IX. Um an Beispielen zu sehen, was (IX.) im Lehrsatz behauptet, setzen wir die nach der obigen Art sich findenden Resultate noch für einige andere z her.

Zweites Beispiel. Es sei

$$43. \quad z = 45 = 3^2.5.$$

Hier ist

$$44. \quad z_\varphi = 1\ 2\ 4\ 7\ 8\ 11\ 13\ 14\ 16\ 17\ 19\ 22\ 23\ 26\ 28\ 29\ 31\ 32\ 34\ 37\ 38\ 41\ 43\ 44,$$

$$45. \quad \varphi z = 24,$$

$$46. \quad r = 1\ 4\ 16\ 19\ 31 \text{ und } 34, \text{ also } \nu = 6 \text{ und } 2n = 4 \text{ (III.)}.$$

Ferner ist für die Gleichung (1.)

$$47. \quad \begin{cases} x_1 = 1\ 19\ 26\ 44 & \text{für } r = 1, \\ x_4 = 2\ \ 7\ 38\ 43 & - \quad r = 4, \\ x_{16} = 4\ 14\ 31\ 41 & - \quad r = 16, \\ x_{19} = 8\ 17\ 28\ 37 & - \quad r = 19, \\ x_{31} = 11\ 16\ 29\ 34 & - \quad r = 31, \\ x_{34} = 13\ 22\ 23\ 32 & - \quad r = 34. \end{cases}$$

Sodann ist für (14.)

$$48. \quad \begin{cases} \varkappa = 1 \quad 3 \quad 5, \\ \lambda = 45 \ 15 \ \ 9, \end{cases}$$

wovon nach (VIII. *a.*) 3 und 15, mit dem Gemeintheiler $3 > 2$, nicht in Betracht kommt.

Für die Gleichung

$$49.\quad (x+1)(x-1) = \mathfrak{S}\varkappa\lambda \ (15.)$$

ist

$$50.\quad \begin{cases} \overset{1}{x} = 1, & \overset{2}{x} = 44 \quad \text{für} \quad \varkappa, \lambda = 1, 45, \\ \overset{1}{x} = 19, & \overset{2}{x} = 26 \quad \text{für} \quad \varkappa, \lambda = 5, \ 9. \end{cases}$$

Drittes Beispiel. Es sei

$$51.\quad z = 126 = 2.3^2.7.$$

Hier ist

$$52.\quad z_\varphi = 1\ 5\ 11\ 13\ 17\ 19\ 23\ 25\ 29\ 31\ 37\ 41\ 43\ 47\ 53\ 55\ 59\ 61$$
$$65\ 67\ 71\ 73\ 79\ 83\ 85\ 89\ 95\ 97\ 101\ 103\ 107\ 109\ 113\ 115\ 121\ 125,$$

$$53.\quad \varphi z = 36,$$

$$54.\quad r = 1\ 25\ 37\ 43\ 67\ 79\ 85\ 109 \text{ und } 121, \text{ also } \nu = 9 \text{ und } 2n = 4 \text{ (III.)}.$$

Ferner ist für die Gleichung (1.)

$$55.\quad \begin{cases} x_1 = 1\ 55\ 71\ 125 & \text{für} \quad r = 1, \\ x_{25} = 5\ 23\ 103\ 121 & - \quad r = 25, \\ x_{37} = 17\ 53\ 73\ 109 & - \quad r = 37, \\ x_{43} = 13\ 41\ 85\ 113 & - \quad r = 43, \\ x_{67} = 47\ 61\ 65\ 79 & - \quad r = 67, \\ x_{79} = 31\ 59\ 67\ 95 & - \quad r = 79, \\ x_{85} = 29\ 43\ 83\ 97 & - \quad r = 85, \\ x_{109} = 19\ 37\ 89\ 107 & - \quad r = 109, \\ x_{121} = 11\ 25\ 101\ 115 & - \quad r = 121. \end{cases}$$

Sodann ist für (14.)

$$56.\quad \begin{cases} \varkappa = 1\ \ 2\ \ 3\ \ 6\ \ 7\ \ 9, \\ \lambda = 126\ 63\ 42\ 21\ 18\ 14; \end{cases}$$

wovon nach (VIII. *a.*) die Factorenpaare 3, 42 und 6, 21, mit dem Gemeintheiler $3 > 2$, nicht in Betracht kommen.

Für die Gleichung

$$57.\quad (x+1)(x-1) = \mathfrak{S}\varkappa\lambda \ (15.)$$

ist

$$58.\quad \begin{cases} \overset{1}{x} = 1, & \overset{2}{x} = 126 \quad \text{für} \quad \varkappa, \lambda = 1, 126, \\ \overset{1}{x} = 1, & \overset{2}{x} = 126 \quad - \quad \varkappa, \lambda = 2, 63, \\ \overset{1}{x} = 55, & \overset{2}{x} = 71 \quad - \quad \varkappa, \lambda = 7, 18, \\ \overset{1}{x} = 55, & \overset{2}{x} = 71 \quad - \quad \varkappa, \lambda = 9, 14. \end{cases}$$

Viertes Beispiel. Es sei

$$59. \quad z = 120 = 2^3.3.5.$$

Hierin ist

$$60. \quad z_\varphi = 1\ 7\ 11\ 13\ 17\ 19\ 23\ 29\ 31\ 37\ 41\ 43\ 47\ 49\ 53\ 59\ 61\ 67\ 71\ 73\ 77\ 79\ 83\ 89\ 91\ 97\ 101\ 103\ 107\ 109\ 113 \text{ und } 119,$$

$$61. \quad \varphi z = 32,$$

$$62. \quad r = 1 \text{ und } 49, \text{ also } \nu = 2 \text{ und } 2n = 16 \text{ (III.)}.$$

Ferner ist für die Gleichung (1.)

$$63. \begin{cases} x_1 = 1\ 11\ 19\ 29\ 31\ 41\ 49\ 59\ 61\ 71\ 79\ 89\ 91\ 101\ 109 \text{ und } 119 \text{ für } r = 1, \\ x_{49} = 7\ 13\ 17\ 23\ 37\ 43\ 47\ 53\ 67\ 73\ 77\ 83\ 97\ 103\ 107 \text{ und } 113 \text{ für } r = 49. \end{cases}$$

Sodann ist für (14.)

$$64. \begin{cases} \varkappa = 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 8\ 10, \\ \lambda = 120\ 60\ 40\ 30\ 24\ 20\ 15\ 12, \end{cases}$$

von welchen Factorenpaaren 1, 120; 3, 40; 5, 24 und 8, 15 *theilerfremd* sind, 2, 60; 4, 30; 6, 20 und 10, 12 hingegen 2 zum Gemeintheiler haben.

Für die Gleichung

$$65. \quad (x+1)(x-1) = \mathfrak{S}\varkappa\lambda \text{ (15.)}$$

ist

$$66. \begin{cases} \overset{1}{x} = 1, & \overset{2}{x} = 119 & \text{für } \varkappa, \lambda = 1, 120, \\ \overset{1}{x} = 41, & \overset{2}{x} = 79 & - \quad \varkappa, \lambda = 3, 40, \\ \overset{1}{x} = 49, & \overset{2}{x} = 71 & - \quad \varkappa, \lambda = 5, 24, \\ \overset{1}{x} = 31, & \overset{2}{x} = 89 & - \quad \varkappa, \lambda = 8, 15; \end{cases}$$

$$67. \begin{cases} \overset{1}{x} = 1, & \overset{2}{x} = 59, & \overset{3}{x} = 61, & \overset{4}{x} = 119 & \text{für } \varkappa, \lambda = 2, 60, \\ \overset{1}{x} = 29, & \overset{2}{x} = 31, & \overset{3}{x} = 89, & \overset{4}{x} = 91 & - \quad \varkappa, \lambda = 4, 30, \\ \overset{1}{x} = 19, & \overset{2}{x} = 41, & \overset{3}{x} = 79, & \overset{4}{x} = 101 & - \quad \varkappa, \lambda = 6, 20, \\ \overset{1}{x} = 11, & \overset{2}{x} = 49, & \overset{3}{x} = 71, & \overset{4}{x} = 109 & - \quad \varkappa, \lambda = 10, 12. \end{cases}$$

An diesen verschiedenen Beispielen wird nun was (IX.) behauptet wie folgt zu sehen sein.

a. $z = 45$ im *zweiten Beispiel* geht *nicht* mit 2 auf, also auch kein $\varkappa$ und λ (48.), und die zu den *theilerfremden* $\varkappa$ und λ 1, 45 und 5, 9 gehörigen Werthe 1, 44, 19 und 26 von x (50.) sind *alle*, die es nach (46.) für x_1 giebt; gemäfs (IX. *a.*).

b. Im *dritten Beispiel* geht $z = 126$ mit 2, und nur mit 2^1 auf. Von den *Factorenpaaren* $\varkappa$ und $\lambda = 1, 126$; 2, 63; 7, 18 und 9, 14 (56.), die

hier in Betracht kommen, geht *ein* Factor mit 2 und mit keiner höhern Potenz von 2 auf, und die zu der ***Hälfte*** dieser Factorenpaare 1, 126 und 7, 18 gehörigen Werthe 1, 125, 55 und 71 von x (58.) sind *alle,* die es nach (55.) für x_1 giebt; gemäfs (IX. *b.*). Die andern beiden Factorenpaare 2, 63 und 9, 14 sind die $\frac{1}{2}\varkappa$ und 2λ der vorigen und geben, wie es nach (VIII. *c.*) sein mufs, *dieselben x.*

Ferner zeigt sich noch was (VIII. *d.*) behauptet auch an dem *vierten Beispiel.* Die Werthe von x für $\varkappa, \lambda = 1, 120$ sind unter denen für $2\varkappa$ und $\frac{1}{2}\lambda = 2, 60$ mitbegriffen u. s. w.

c. Das *erste* und das *vierte* Beispiel sind in dem Falle (IX. *c.*). z geht mit einer höhern als der ersten Potenz von 2 auf, und es giebt Factorenpaare, die *beide* mit 2 aufgehen.

Im *ersten* Beispiel nun sind die Werthe 19, 71, 109, 161, 1, 89, 91 und 179 von x, die in (39.) zu den Factorenpaaren 10, 18 und 2, 90 gehören, welche 2 zum Gemeintheiler haben, schon *alle,* die es nach (25. 1.) giebt, und die zu den *theilerfremden* Factorenpaaren 5, 36; 1, 180; 4, 45; 9, 20 gehörigen Werthe von x (37.) sind *dieselben.*

Im *vierten* Beispiel sind die Werthe von x, welche in (67.) zu den mit 2 gemeintheilbaren Factorenpaaren 2, 6; 4, 30; 6, 20 und 10, 12 gehören, *alle sechzehn,* die es nach (63.) giebt, und die zu den *theilerfremden* Factorenpaaren 1, 120; 3, 40; 5, 24 und 8, 15 nach (66.) gehörigen *acht* Werthe von x sind unter ihnen mitbegriffen; gemäfs (IX. *c.*).

Beweis von I. *A.* Könnte ein und derselbe Werth von x in $x^2 = \mathfrak{G}z + r$ (1.) verschiedene r geben, so müfste z. B. $x^2 = \mathfrak{G}z + r_1$, und *zugleich* $x^2 = \mathfrak{G}z + r_2$, also, Eins vom andern abgezogen,

$$68. \quad \mathfrak{G}z = r_1 - r_2$$

sein, folglich $r_1 - r_2$ mit z *aufgehen.* Dies kann nicht sein, da r_1 und r_2 beide $< z$ sind, und also auch $r_1 - r_2 < z$ ist. Also gehören nothwendig zu *andern* Werthen von r *andere x;* gemäfs (I.).

Beweis von II. und III. *B.* Die Gleichung $x_1^2 = \mathfrak{G}z + 1$ (2.), mit *irgend einem* der Werthe von x_r, die der Gleichung $x_r^2 = \mathfrak{G}z + r$ (1.) genugthun, multiplicirt, giebt

$$69. \quad x_1^2 . x_r^2 = \mathfrak{G}z + r.$$

Setzt man nun wie in (3.)

$$70. \quad x_1 . x_r = \mathfrak{G}z + (x_r),$$

so giebt (69.)

$$(\mathfrak{S}z+(x_r))^2 = \mathfrak{S}z+r \text{ oder}$$

$$71. \quad (x_r)^2 = \mathfrak{S}z+r:$$

also thut (x_r) der Gleichung $x_r^2 = \mathfrak{S}z+r$ (1.) genug, und folglich ist (x_r) nothwendig ***einer der Werthe*** von x_r.

C. Zu jedem ***andern*** x_1, und für ***dasselbe*** x_r, gehört aber in (70.) nothwendig ein ***anderes*** (x_r). Denn gäben z. B. die zwei Werthe $\overset{1}{x}_1$ und $\overset{2}{x}_1$ von x_1 in (70.) ***ein- und dasselbe*** (x_r), so müfste $\overset{1}{x}_1 x_r = \mathfrak{S}z+(x_r)$ und ***zugleich*** $\overset{2}{x}_1 x_r = \mathfrak{S}z+(x_r)$ und, Eins vom Andern abgezogen,

$$72. \quad (\overset{1}{x}_1-\overset{2}{x}_1)x_r = \mathfrak{S}z$$

sein, folglich $(\overset{1}{x}_1-\overset{2}{x}_1)x_r$ mit z ***aufgehen;*** was nicht sein kann, da x_r zu z ***theilerfremd*** ist, folglich keinen der Factoren von z, >1 mit z gemein hat, in $\overset{1}{x}_1-\overset{2}{x}_1$ ***allein*** aber z nicht aufgehen kann, da $\overset{1}{x}_1$ und $\overset{2}{x}_1$ beide $<z$ sind, und also auch $\overset{1}{x}_1 = \overset{2}{x}_1 < z$ ist. Daher gehört zu jedem ***andern*** x_1 für ***dasselbe*** x_r nothwendig ein ***anderes*** (x_r), und folglich giebt es nothwendig ***wenigstens*** eben so viele verschiedene x_r als es verschiedene x_1 giebt, mithin ihrer ***wenigstens*** $2n$.

D. Es kann ihrer aber auch ***nicht mehr*** geben. Denn die x_r für die verschiedenen ν Werthe von r sind zusammengenommen ***alle*** die φz zu z theilerfremden Zahlen $z_\varphi > 0$ und $< z$, und jedes z_φ kommt ***nur einmal*** vor; denn die verschiedenen ν Reste r gehen eben daraus hervor, dafs man das x in (1.) alle die φz Zahlen z_φ durchlaufen läfst. Berührte nun x_r für ein- und dasselbe r ***mehr*** als $2n$ Werthe von z_φ, so müfste x_r für ein ***anderes*** r nothwendig ***weniger*** als $2n$ verschiedene Werthe haben, indem, wenn es anders wäre, die x_r für die zwei verschiedenen r ein- und dasselbe z_φ zweimal berühren würden; was nicht sein kann. Und da es nun für kein r ***weniger*** als $2n$ verschiedene Werthe geben kann, so kann es deren auch ***nicht mehrere*** geben. Folglich giebt es für ***jeden*** der ν Werthe von r nothwendig $2n$ verschiedene Werthe von $x = z_\varphi$, die auch für die ***verschiedenen*** r nach (I.) alle verschieden sind, gemäfs (II.), und es ist

$$73. \quad \varphi z = 2n\nu;$$

gemäfs (III. 4.).

Beweis von IV. ***E.*** Man setze für die zwei verschiedenen Werthe r_1 und r_2 von r,

$$74.\quad x_{r_1}^2 = \mathfrak{G}z + r_1 \quad\text{und}\quad x_{r_2}^2 = \mathfrak{G}z + r_2,$$

so ergiebt sich, wenn man diese beiden Gleichungen in einander multiplicirt,

$$75.\quad x_{r_1}^2 . x_{r_2}^2 = \mathfrak{G}z + r_1 r_2,$$

und wenn man

$$76.\quad r_1 r_2 = \mathfrak{G}z + r_\lambda \quad\text{und}\quad x_{r_1} . x_{r_2} = \mathfrak{G}z + x_{r_\lambda}$$

setzt, aus (75.)

$$(\mathfrak{G}z + x_{r_\lambda})^2 = \mathfrak{G}z + r_1 r_2 = \mathfrak{G}z + \mathfrak{G}z + r_\lambda \quad\text{oder}$$

$$77.\quad x_{r_\lambda}^2 = \mathfrak{G}z + r_\lambda.$$

Also ist der aus dem ***Product*** $r_1 r_2$ der Quadratreste r_1 und r_2 nach (76.) hervorgehenden Rest r_λ ebenfalls ein ***Quadratrest.***

F. Multiplicirt man r_λ von neuem mit einem Quadratrest, so geht, vermöge ***derselben*** Gründe, aus dem Product wieder ein Quadratrest hervor. Und so weiter. Also ist für eine beliebige Zahl von Quadratresten:

$$78.\quad r_1 r_2 r_3 \ldots r_\alpha = \mathfrak{G}z + r_\mu;$$

gemäfs (5. 1.).

G. Der Beweis bleibt derselbe, wenn auch die in einander multiplicirten Reste r ***einander gleich*** sind; also ist auch

$$79.\quad r^\tau = \mathfrak{G}z + r_\mu;$$

gemäfs (5. 2.).

Beweis von V. ***H.*** Da nach (IV.) ***jede Potenz*** eines der Quadratreste r wieder einen der Quadratreste r giebt, so ist für einen beliebigen positiven ganzzahligen Exponenten λ,

$$80.\quad r^\lambda = \mathfrak{G}z + r_\lambda.$$

I. Gesetzt nun, für ***keinen*** der Werthe 2, 3, 4, ... von λ sei r_λ ***gleich*** r, so durchläuft r_λ ***alle*** die Werthe, welche r haben ***kann.*** Aber r hat nur ν verschiedene Werthe, also mufs jedenfalls für die $\nu+1$te Potenz das erste r_1 ***wiederkehren,*** und folglich mufs

$$81.\quad r^{\nu+1} = \mathfrak{G}z + r \text{ sein.}$$

Daraus folgt, dafs $\mathfrak{G}z$, und zwar $\mathfrak{G}$ (weil z zu r ***theilerfremd*** ist) mit r ***aufgehen*** mufs; folglich ergiebt sich, wenn man mit r dividirt,

$$82.\quad r^\nu = \mathfrak{G}z + 1, \quad\text{oder}\quad r^{\frac{\varphi z}{2n}} = \mathfrak{G}z + 1;$$

gemäfs (6. und 7.).

K. Aber es kann allerdings schon für $\lambda < \nu + 1$ in (80.) $r_\lambda = r$ sein. Z. B. schon für $\lambda = 3$ kann in

$$83.\quad r^3 = \mathfrak{G}z + r_\lambda \text{ (80.)}$$

$r_\lambda = r$ sein. Denn alsdann giebt (83.), durch r_λ dividirt,

$$84.\quad r^2 = \mathfrak{S}z + 1,$$

und was vorausgesetzt wird gilt also in der That von jedem r, welches eine der *Quadratwurzeln* für z zu 1 ist, wie z. B. $r = 109$ in (25.), welches nach (25. 1.) $109^2 = \mathfrak{S}z + 1$ giebt.

Selbst schon für $\lambda = 2$ kann in (80.), also in

$$85.\quad r^2 = \mathfrak{S}z + r_\lambda \ (80.)$$

$r_\lambda = r$ sein. Denn alsdann giebt (85.), durch $r = r_\lambda$ dividirt,

$$86.\quad r = \mathfrak{S}z + 1;$$

und dies ist für den Werth 1 von r der Fall. Also auch schon eine *niedrigere* als die νte Potenz von r kann zu z den Rest 1 lassen. *Jedenfalls* aber ist $r^\nu = \mathfrak{S}z + 1$; gemäfs (V.).

Beweis von VI. *L.* Wenn man (8.) mit r^2 multiplicirt, so ergiebt sich

$$87.\quad r^2 x_1^2 = \mathfrak{S}z + r^2.$$

Hierin (9.) und (10.) gesetzt giebt

$$(\mathfrak{S}z + (x))^2 = \mathfrak{S}z + \mathfrak{S}z + \overset{1}{\underset{1}{r}} \text{ oder}$$

$$88.\quad (x)^2 = \mathfrak{S}z + r.$$

Dieses ist die Gleichung (11.); und zwar giebt vermöge (10.) jedes *andere* r für (11. oder 90.) ein *anderes* (x); gemäfs (VI.).

Beweis von VII. In

$$89.\quad x^2 = \mathfrak{S}z + r$$

giebt, $z - x$ statt x gesetzt, wie schon weiter oben bemerkt, *dasselbe* r. Geht nun z mit 2 auf, so dafs $\frac{1}{2}z$ eine *ganze* Zahl ist, so ist

$$90.\quad (\tfrac{1}{2}z \pm x)^2 = \tfrac{1}{4}z^2 \pm zx + x^2.$$

Hierin (89.) gesetzt, giebt

$$(\tfrac{1}{2}z \pm x)^2 = \tfrac{1}{4}z^2 \pm zx + \mathfrak{S}z + r \text{ oder}$$

$$91.\quad (\tfrac{1}{2}z \pm x)^2 = \mathfrak{S}z + r.$$

Also auch $\frac{1}{2}z + x$ und $\frac{1}{2}z - x$ geben zu z *denselben* Rest r, welchem x entspricht, und folglich geben

$$92.\quad x,\ \tfrac{1}{2}z - x,\ \tfrac{1}{2}z + x \text{ und } z - x$$

sämmtlich zu z *denselben Quadratrest* r, sobald z mit 2 aufgeht; gemäfs (VII.).

Beweis von VIII. *N.* Wenn man, wie in (14.),

$$93.\quad z = \varkappa\lambda$$

setzt und sich in der Gleichung

94. $(x+1)(x-1) = \mathfrak{S}\varkappa\lambda$ (15.)

$\mathfrak{S}\varkappa\lambda$ *zusammen* in alle seine gleichen und ungleichen *Stammtheiler* zerlegt vorstellt, so mufs nothwendig $x+1$ dem Product einer gewissen Anzahl derselben, und $x-1$ dem Product *aller übrigen* gleich sein.

Bezeichnet man das unbekannte $\mathfrak{S}$ durch

95. $\mathfrak{S} = \varkappa_1\lambda_1$,

so dafs in (94.)

96. $(x+1)(x-1) = \varkappa\lambda.\varkappa_1\lambda_1$

ist, so kann man immer

97. $x+1 = \varkappa\lambda_1$ und

98. $x-1 = \lambda\varkappa_1$

setzen.

In der That drücken (97. und 98.) *alle möglichen* Fälle aus. Es kann nemlich nicht, da x immer $< z$ sein soll (wenigstens um 1), $x+1$, und noch weniger $x-1$, *gröfser* als $z = \varkappa\lambda$ sein: also kann niemals $x+1 = \varkappa\lambda.\varkappa_1$ oder $= \varkappa\lambda.\lambda_1$ gesetzt werden müssen, wo $\varkappa_1$ oder $\lambda_1 > 1$ ist. Blofs wenn $x = z-1$ ist, ist $x+1 = z = \varkappa\lambda$ und $x-1 = z-2$. Aber auch diesen Fall drücken (97. und 98.) aus; denn es ist für denselben dann in (97.) $\lambda_1 = \lambda$, also in (98.) $x-1 = \lambda_1\varkappa_1$, wie (95.). Für jedes andere $x < z-1$ ist nothwendig sowohl $x+1$ als $x-1 < \varkappa\lambda$ $(= z)$.

Es kann nun zwar für ein $x < z-1$, $x+1$ z. B. blofs einem der Factoren von z allein gleich sein, z. B. $x+1 = \varkappa$, welches der Fall sein würde, wenn $x+1$ in $z = \varkappa\lambda$ allein aufgeht. Aber auch diesen Fall drücken (97. und 98.) aus; denn dann ist in (97.) $\lambda_1 = 1$, also in (95.) $\varkappa_1 = \mathfrak{S}$ und in (98.) $x-1 = \lambda\mathfrak{S}$, und wie gehörig $(x+1)(x-1) = \varkappa\lambda\mathfrak{S}$.

Es kann ferner nicht $x+1$ in $\mathfrak{S}$ allein aufgehen, oder auch $= \mathfrak{S}$ sein, denn sonst wäre zufolge (94.) $x-1 > \varkappa\lambda$ oder $x-1 = \varkappa\lambda$, also $x > \varkappa\lambda > z$; gegen die Voraussetzung. Immer ist $\mathfrak{S} < z$, und es kann nicht $x+1$ blofs Factoren von $\mathfrak{S}$ wegnehmen, auch nicht alle, weil dann für das *kleinere* $x-1$ das *gröfsere* z übrig bleiben würde. Es mufs $x+1$ auch noch Factoren *von* z in Anspruch nehmen; und zwar mufs es entweder in z allein aufgehen, welches der obige Fall $\lambda_1 = 1$ ist, oder es mufs $= z$ sein, welches der Fall $x = z-1$ ist, oder es mufs einen Theil seiner Factoren aus z und die übrigen, mit λ_1 bezeichneten, aus $\mathfrak{S}$ nehmen.

Es kann nun zwar, wenn man die Factoren $\varkappa$ und λ im *voraus bestimmt*, sein, dafs es *kein* x giebt, welches durch $x+1$ gerade den einen

vorausbestimmten Factor von z, z. B. $\varkappa$, und etwa aufserdem einen Factor λ_1 von $\mathfrak{G}$ wegnimmt: aber es kann *nicht* sein, dafs es für einen Werth von x, der die Gleichung $x^2 = \mathfrak{G}z + 1$ oder $(x+1)(x-1) = \mathfrak{G}z$ wirklich erfüllt, nicht irgend einen Factor von z, z. B. $\varkappa$, gäbe, der mit irgend einem Factor λ_1 von $\mathfrak{G}$ zusammen, sei auch dieser letztere $= 1$, $x+1$ ausmacht; denn wenn x wirklich eine *ganze* Zahl ist, so mufs *nothwendig* $x+1$ in $\mathfrak{G}z$ *aufgehen* und zum Quotienten $x-1$ geben, also nothwendig von den möglichen Factoren $\varkappa$ und λ von z diese oder jene in Anspruch nehmen. Also wenn man *alle* x, welche Statt finden, durchgeht, so kann es zwar sein, dafs *nicht alle Factoren* $\varkappa$ und λ von z durch die Gleichung $(x+1)(x-1) = \mathfrak{G}\varkappa\lambda$ berührt werden, aber es kann *nicht sein*, dafs es, wenn man die *Factoren* $\varkappa$ und λ von z *alle* ganzzahligen Werthe durchlaufen läfst, die sie haben *können*, *nicht irgend ein* x *gäbe*, welches darunter nicht für die Gleichung $(x+1)(x-1) = \mathfrak{G}\varkappa\lambda$ das für ihn passende $\varkappa$ und λ fände.

So passen denn also die Ausdrücke (97. und 98.) für *alle* Fälle, und die Bedingung in (VIII.), dafs $x+1$ mit dem einen der Factoren $\varkappa$ und λ, $x-1$ mit dem andern *aufgehe*, das heifst, dafs, wie (97. und 98.) es annimmt, $x+1 = \varkappa\lambda_1$ und $x-1 = \lambda\varkappa_1$ sei, ist nicht blofs *willkürlich*, sondern *nothwendig*.

Es kommt nur darauf an, in (97. und 98.) die *Factoren* $\varkappa$ und λ von z *alle* Werthe, welche sie haben *können*, durchlaufen zu lassen, um nothwendig durch (97. und 98.) *alle* ganzzahligen Werthe von $x < z$ zu finden, die *möglich* sind, das heifst, die die Gleichung

$$99. \quad x^2 = \mathfrak{G}z + 1$$

erfüllen.

Giebt man nun, um die x zu finden, auf diese Weise den $\varkappa$ und λ der Reihe nach diese oder jene bestimmten Werthe, aus denen, welche sie haben können, so lassen sich vermittels der Gleichungen (97. und 98.) die zugehörigen Werthe von x wie folgt finden; insbesondere also auch die *Anzahl* der x, auf welche *Anzahl* es hier allein ankommt.

O. Man subtrahire und addire die beiden Gleichungen (97 und 98.), so geben sie $2 = \varkappa\lambda_1 - \lambda\varkappa_1$ oder

$$100. \quad \varkappa\lambda_1 = \lambda\varkappa_1 + 2 \text{ und}$$

$$101. \quad 2x = \varkappa\lambda_1 + \lambda\varkappa_1.$$

P. Aus (100.) folgt, dafs $\varkappa$ und λ keinen Theiler $\delta > 2$ gemein haben können, denn jeder Gemeintheiler δ von $\varkappa$ und λ mufs zufolge (100.)

nach (§. 18.) auch in die Zahl 2 rechts aufgehen, und in diese Zahl geht keine Zahl $\delta > 2$ auf. Daraus folgt, dafs für jedes Factorenpaar $\varkappa$ und λ von z, welches einen *gröfsern* Gemeintheiler als 2 hat, die Gleichung (100.) nicht möglich ist, und dafs es also dann gar keine ganzzahligen Werthe von $\varkappa_1$ und λ_1, und folglich auch gar keine dazu gehörigen Werthe von x giebt. Dieses ist was (VIII. *a.*) behauptet.

Haben dagegen $\varkappa$ und λ nur 1 und 2 zum *Gemeintheiler,* so können die Gleichungen (100. und 101.), wie sich zeigen wird, Statt finden, und es giebt zugehörige Werthe von x.

Q. Man setze nemlich zuerst, $\varkappa$ und λ seien *theilerfremd* oder hätten nur 1 zum *Gemeintheiler,* so bleibt die Gleichung (100.) wie sie ist, und nach (§. 34. III.) giebt es immer *einen und nur einen* Werth von $\lambda_1 > 0$ und $< \lambda$, und *einen und nur einen* Werth von $\varkappa_1 > 0$ und $< \varkappa$, welche die Gleichung (100.) erfüllen. Sie mögen durch $\varkappa_0$ und λ_0 bezeichnet werden. Desgleichen giebt es nach (§. 34. II.) noch unzählige andere Werthe von $\varkappa_1$ und λ_1, die alle durch

$$102. \quad \varkappa_1 = n\varkappa + \varkappa_0 \text{ und}$$

$$103. \quad \lambda_1 = n\lambda + \lambda_0$$

ausgedrückt werden, wo n eine *beliebige* positive oder negative ganze Zahl, aber für $\varkappa_1$ und für λ_1 die *nemliche* ist.

Setzt man nun die Ausdrücke von $\varkappa_1$ und λ_1 (102. und 103.) in den Ausdruck von $2x$ (101.), so ergiebt sich $2x = n\varkappa\lambda + \varkappa\lambda_0 + n\varkappa\lambda + \lambda\varkappa_0$, oder da $\varkappa\lambda = z$ ist (93.),

$$104. \quad 2x = 2nz + \varkappa\lambda_0 + \lambda\varkappa_0.$$

Was nun auch $\varkappa_0$ und λ_0 sein mögen: man weifs, dafs $\varkappa_0 > 0$ und $< \varkappa$ und $\lambda_0 > 0$ und $< \lambda$ ist, woraus folgt, dafs $\varkappa\lambda_0 + \lambda\varkappa_0$ jedenfalls > 0 und $< \varkappa\lambda + \varkappa\lambda$ also $< 2z$ ist.

Hieraus, und dann daraus, dafs der Werth von x *zeichenfrei* > 0 und $< z$ sein mufs (*negativ* kann nemlich x in der Gleichung $x^2 = \mathfrak{G}z + 1$ (99.) allerdings sein; positive und negative x von gleich grofsen zeichenfreien Werthen erfüllen die Gleichung gleichmäfsig), folgt weiter, dafs in (104.) das willkürliche n *nur* 0 und -1 sein kann. Denn $n = 1$ giebt, da $\varkappa\lambda_0 + \lambda\varkappa_0 > 0$ und $< 2z$ ist, $2x > 2z$, also $x > z$, und $n < -1$, z. B. schon $n = -2$, giebt $2x = -4z + \varkappa\lambda_0 + \lambda\varkappa_0$, also ein x, dessen zeichenfreier Werth ebenfalls $> z$ ist.

Es giebt demnach in (104.) *nur zwei* Werthe von x, und diese, zu $n=0$ und $n=-1$ gehörig, sind, wenn man sie durch $\overset{1}{x}$ und $\overset{2}{x}$ bezeichnet,

$$105. \quad \overset{1}{x} = \tfrac{1}{2}(\varkappa\lambda_0 + \lambda\varkappa_0) \text{ und}$$

$$106. \quad \overset{2}{x} = z - \tfrac{1}{2}(\varkappa\lambda_0 + \lambda\varkappa_0) = z - \overset{1}{x},$$

wo $\varkappa_0$ und λ_0 aus der Gleichung (100.) zu berechnen sind.

Nur die zwei Werthe $\overset{1}{x}$ und $z-\overset{1}{x}$ also können für ein *theilerfremdes* Factorenpaar $\varkappa$ und λ von z Statt finden; und dies ist was (VIII. *b.*) behauptet.

R. Man setze jetzt den *zweiten* nach (***P.***) möglichen Fall, nemlich, dafs $\varkappa$ und λ den *Gemeintheiler* 2 haben.

Alsdann reduciren sich die Gleichungen (100. und 101.), da sie nun beide mit 2 dividirt werden können, auf

$$107. \quad \tfrac{1}{2}\varkappa\lambda_1 = \tfrac{1}{2}\lambda\varkappa_1 + 1 \text{ und}$$

$$108. \quad x = \tfrac{1}{2}\varkappa\lambda_1 + \tfrac{1}{2}\lambda\varkappa_1.$$

Wie in (***Q.***) giebt es wieder nach (§. 34. III.) *einen und nur einen Werth* von $\lambda_1 > 0$ und hier $< \frac{1}{2}\lambda$, und *einen und nur einen* Werth von $\varkappa_1 > 0$ und hier $< \frac{1}{2}\varkappa$, welche der Gleichung (107.) genugthun und welche wieder durch $\varkappa_0$ und λ_0 bezeichnet werden mögen. Desgleichen giebt es nach (§. 34. III.) noch unzählige andere Werthe von $\varkappa_1$ und λ_1, die alle durch

$$109. \quad \varkappa_1 = n.\tfrac{1}{2}\varkappa + \varkappa_0 \text{ und}$$

$$110. \quad \lambda_1 = n.\tfrac{1}{2}\lambda + \lambda_0$$

ausgedrückt werden, wo n eine *beliebige* positive oder negative ganze Zahl aber für $\varkappa_1$ und λ_1 die *nemliche* ist.

Setzt man nun wieder die Ausdrücke von $\varkappa_1$ und λ_1 (109. und 110.) in den Ausdruck von x (108.), so ergiebt sich $x = n.\frac{1}{2}\varkappa.\frac{1}{2}\lambda + \frac{1}{2}\varkappa\lambda_0 + n.\frac{1}{2}\lambda.\frac{1}{2}\varkappa + \frac{1}{2}\lambda\varkappa_0$, oder, da $\varkappa\lambda = z$ ist (93.)

$$111. \quad x = \tfrac{1}{2}nz + \tfrac{1}{2}(\varkappa\lambda_0 + \lambda\varkappa_0).$$

Was nun auch $\varkappa_0$ und λ_0 sein mögen: man weifs dafs $\varkappa_0 > 0$ und $< \frac{1}{2}\varkappa$ und $\lambda_0 > 0$ und $< \frac{1}{2}\lambda$ ist, woraus folgt, dafs $\frac{1}{2}(\varkappa\lambda_0 + \lambda\varkappa_0)$ jedenfalls > 0 und $< \frac{1}{2}\varkappa\lambda$ oder $< \frac{1}{2}z$ ist.

Hieraus, und dann daraus, dafs der Werth von x *zeichenfrei* > 0 und $< z$ sein mufs, folgt vermöge (111.) weiter, dafs z nur die vier Werthe -2, -1, 0 und $+1$ haben kann. Bezeichnet man nemlich den zu $n=0$ gehörigen positiven Werth von x durch $\overset{1}{x}$, die andern Werthe von x für $n=-1$, $n=+1$ und $n=-2$ durch $\overset{2}{x}$, $\overset{3}{x}$, $\overset{4}{x}$, so giebt (111.)

$$112.\quad\begin{cases} 1.\ \overset{1}{x} = \tfrac{1}{2}(\varkappa\lambda_0 + \lambda\varkappa_0) & \text{für } n = 0, \\ 2.\ \overset{2}{x} = -\tfrac{1}{2}z + \overset{1}{x} & \text{für } n = -1, \\ 3.\ \overset{3}{x} = +\tfrac{1}{2}z + \overset{1}{x}, & \text{für } n = +1, \\ 4.\ \overset{4}{x} = -\ z + \overset{1}{x}, & \text{für } n = -2. \end{cases}$$

Von allen diesen vier x sind die Werthe, da $x < \frac{1}{2}z$ ist, zeichenfrei genommen, > 0 und $< z$; wie es sein soll. Aber schon $n = +2$ und $n = -3$ giebt

$$113.\quad x = z + \overset{1}{x} \quad\text{und}\quad x = -\tfrac{3}{2}z + \overset{1}{x},$$

wovon die Werthe zeichenfrei $> z$ sind und also nicht Statt finden.

Die Werthe (112.) von x sind nun, zeichenfrei genommen, diejenigen (17. und 18.), und also giebt es für jedes Factorenpaar $\varkappa$ und λ von z, welches den Gemeintheiler 2 hat, wie es (VIII. *e.*) behauptet, ***vier*** Werthe von x oder ***zwei Werthenpaare*** dieser Gröfsen für die Gleichung $x^2 = \mathfrak{G}z + 1$. In den Ausdrücken derselben (112.) müssen $\varkappa$ und λ, aus der Gleichung (107.) berechnet werden.

S. Wir haben bis hieher gefunden, dafs es für jedes ***bestimmte*** Factorenpaar $\varkappa$ und λ von z entweder ***ein*** oder ***zwei*** Werthenpaare von x giebt, die der Gleichung $x^2 = \mathfrak{G}z + 1$ genugthun: ersteres wenn $\varkappa$ und λ ***theilerfremd*** sind, letzteres wenn $\varkappa$ und λ die Zahl 2 zum ***Gemeintheiler*** haben; und ***nur*** diese beiden Fälle können vorkommen.

Aber es kommt noch darauf an, ob und in wiefern ***verschiedene bestimmte*** Factorenpaare von z, z. B.

$$114.\quad \varkappa\lambda = z \quad\text{und}$$

$$115.\quad \sigma\tau = z$$

dieselben Werthe von x geben können; denn da der Zweck ist, die ***Anzahl*** der ***überhaupt*** für ein gegebenes z möglichen ***verschiedenen Werthenpaare*** von x, die die Gleichung $x^2 = \mathfrak{G}z + 1$ erfüllen, zu finden, und zwar eben aus den verschiedenen Factorenpaaren, in welche sich z zerlegen läfst, so mufs man nothwendig wissen, ***welche*** verschiedene bestimmte Factorenpaare von z, z. B. $\varkappa$ und λ, oder σ und τ, ***dieselben*** Werthe von x geben, um diese Werthe von x, wenn man die Factorenpaare von z ***zählt,*** nicht doppelt oder mehrfach zu zählen.

T. *a.* Man setze zu dem Ende $\sigma\tau = z$ (115.) gebe die ***nemlichen*** x wie $\varkappa\lambda = z$ (114.). Alsdann mufs, wenn man für $z = \sigma\tau$ in $x^2 = \mathfrak{G}z + 1$, ähnlich wie in (93.) für $z = \varkappa\lambda$,

$$116.\quad \mathfrak{S} = \sigma_1\tau_1$$

setzt mit (97. und 98.) *zugleich*

$$117.\quad x+1 = \sigma\tau_1 \text{ und}$$

$$118.\quad x-1 = \tau\sigma_1;$$

also vermöge (97. und 117.) und (98. und 118.)

$$119.\quad \sigma\tau_1 = \varkappa\lambda_1 \text{ und}$$

$$120.\quad \tau\sigma_1 = \lambda\varkappa_1$$

sein, während zugleich vermöge (114. und 115.)

$$121.\quad \sigma\tau = \varkappa\lambda$$

ist. Desgleichen mufs *zugleich* mit

$$122.\quad \varkappa\lambda_1 = \lambda\varkappa_1 + 2 \text{ (100.)}$$

vermöge (117. und 118.)

$$123.\quad \sigma\tau_1 = \tau\sigma_1 + 2 \text{ sein.}$$

b. Nun setze man, der *gröfste Gemeintheiler* von $\varkappa$ und σ sei δ, von λ und τ aber ε, und es sei

$$124.\quad \varkappa = k\delta,\quad \lambda = l\varepsilon,$$

$$125.\quad \sigma = s\delta,\quad \tau = t\varepsilon;$$

so sind k und s, und l und t nothwendig *theilerfremd*.

c. Man setze die Ausdrücke von $\varkappa$ und λ, σ und τ in (121.), so ergiebt sich $k\delta l\varepsilon = s\delta t\varepsilon$ oder

$$126.\quad kl = st,$$

und daraus folgt, weil k und s, l und t *theilerfremd* sind, dafs *k in t und s in l oder t in k und l in s aufgehen mufs* und folglich vermöge (124. und 125.) auch *k in τ und s in λ, oder t in $\varkappa$ und l in σ.*

d. Man setze eben so die Ausdrücke von $\varkappa$ und λ, σ und τ in (119. und 120.), so ergiebt sich $s\delta\tau_1 = k\delta\lambda_1$ und $t\varepsilon\sigma_1 = l\varepsilon\varkappa_1$ oder

$$127.\quad s\tau_1 = k\lambda_1 \text{ und}$$

$$128.\quad t\sigma_1 = l\varkappa_1.$$

Hieraus folgt, da k und s, l und t *theilerfremd* sind, dafs *s in λ_1, k in τ_1 und t* in $\varkappa_1$, *l in σ_1 aufgehen mufs.*

e. Vermöge (*c.* und *d.*) mufs also k in τ und *zugleich* in τ_1, und s in λ und *zugleich* in λ_1, oder t in $\varkappa$ und *zugleich* in $\varkappa_1$ und l in σ und *zugleich* in σ_1 *aufgehen.*

f. Wenn aber nun k in τ und τ_1 *zugleich* aufgeht, so mufs es vermöge (123.) auch in 2 aufgehen (§. 18.). Wenn s in λ und λ_1 *zugleich* aufgeht, so mufs es vermöge (122.) ebenfalls in 2 aufgehen. Auch l, wenn es

zugleich in $\varkappa$ und $\varkappa_1$ aufgeht, mufs vermöge (122.) in 2 aufgehen. Und l, wenn es in σ und σ_1 ***zugleich*** aufgeht, mufs vermöge (123.) gleichfalls in 2 aufgehen.

Die Zahlen k, l, s, t müssen also *sämmtlich* in 2 aufgehen und können daher nur 1 *oder* 2 sein.

g. Daher kann in (124. und 125.) nur

$$129. \begin{cases} 1.\ \varkappa = \delta, \text{ oder } \varkappa = 2\delta; \\ 2.\ \sigma = \delta, \text{ oder } \sigma = 2\delta; \\ 3.\ \lambda = \varepsilon, \text{ oder } \lambda = 2\varepsilon; \\ 4.\ \tau = \varepsilon, \text{ oder } \tau = 2\varepsilon, \end{cases}$$

also nur

$$130.\quad \sigma = \varkappa \text{ oder } \sigma = \tfrac{1}{2}\varkappa \text{ oder } \sigma = 2\varkappa \text{ und}$$

$$131.\quad \tau = \lambda \text{ oder } \tau = \tfrac{1}{2}\lambda \text{ oder } \tau = 2\lambda$$

sein. Es kann aber nicht ***zugleich*** $\sigma = \frac{1}{2}\varkappa$ und $\tau = \frac{1}{2}\lambda$, auch nicht zugleich $\sigma = 2\varkappa$ und $\tau = 2\lambda$ sein, wenn $\sigma\tau$ ***gleich*** $\varkappa\lambda$ ist (121.). Also kann nur

$$132.\quad \sigma = \varkappa \text{ oder } \sigma = \tfrac{1}{2}\varkappa \text{ oder } \sigma = 2\varkappa$$

und ***zugleich***

$$133.\quad \tau = \lambda \text{ oder } \tau = 2\lambda \text{ oder } \tau = \tfrac{1}{2}\lambda \text{ sein.}$$

h. Haben $\varkappa$ und λ den ***Gemeintheiler*** 2, und setzt man das ***Gleiche*** von σ und τ voraus, so reduciren sich die beiden Gleichungen (122. und 123.) auf

$$134.\quad \tfrac{1}{2}\varkappa.\lambda_1 = \tfrac{1}{2}\lambda.\varkappa_1 + 1 \text{ und}$$

$$135.\quad \tfrac{1}{2}\sigma.\tau_1 = \tfrac{1}{2}\tau.\sigma_1 + 1.$$

Ganz wie in (*c.* und *d.*) folgt, dafs, eben wie (*e.*) es aussagt, $\varkappa$ je in τ und τ_1, s je in λ und λ_1, t je in $\varkappa$ und $\varkappa_1$ und l je in σ und σ_1 ***zugleich*** aufgehen mufs, denn alles dies folgt aus den unverändert bleibenden Gleichungen (121.) und (119. und 120.). Dagegen aber können hier k, s, t und l statt 1 und 2 wie in (*f.*) nur sämmtlich $= 1$ sein, indem jetzt in (134. und 135.) in die Zahl 1 rechterhand, anders wie in die Zahl 2 in (122. und 123.) nur allein 1 aufgeht. Also kann hier, statt wie in (129.), nur allein

$$136.\quad \varkappa = \delta,\ \sigma = \delta \text{ und}$$

$$137.\quad \lambda = \varepsilon,\ \tau = \varepsilon$$

und folglich ***nur***

$$138. \begin{cases} \sigma = \varkappa \text{ und} \\ \tau = \lambda \text{ sein.} \end{cases}$$

i. Es folgt also, zusammengenommen, dafs

Erstlich, wenn $\varkappa$ und λ ***theilerfremd*** sind, nur

$$139.\quad \sigma = \varkappa, \text{ oder } \tfrac{1}{2}\varkappa, \text{ oder } 2\varkappa \text{ und } \textit{zugleich}$$

$$140.\quad \tau = \lambda, \text{ oder } 2\lambda, \text{ oder } \tfrac{1}{2}\lambda \text{ und}$$

Zweitens, wenn $\varkappa$ und λ den *Gemeintheiler* 2 haben, nur allein

$$141. \quad \begin{cases} \sigma = \varkappa \text{ und} \\ \tau = \lambda \end{cases}$$

sein kann. Also, wenn $\varkappa$ und λ *theilerfremd* sind, so giebt es *nur die zwei* von $\varkappa$ und λ *verschiedenen* Factorenpaare von *z*: $\sigma = \frac{1}{2}\varkappa$, $\tau = 2\lambda$ und $\sigma = 2\varkappa$ und $\tau = \frac{1}{2}\lambda$, welchen *dieselben x* zukommen, und keine andern; und wenn $\varkappa$ und λ den *Gemeintheiler* 2 haben, so giebt es *gar keine* von $\varkappa$ und λ verschiedene Factorenpaare von *z* für die *nemlichen x.*

U. Es werden nun die Resultate in (*T.*) auf die verschiedenen Fälle, welche vorkommen können, anzuwenden sein.

a. Sind zuerst $\varkappa$ und λ nicht blofs *theilerfremd,* sondern auch beide *ungerade,* so findet weder $\frac{1}{2}\varkappa$ noch $\frac{1}{2}\lambda$ Statt, und daher kann in (139. und 140.) *blofs* $\sigma = \varkappa$ und $\tau = \lambda$ sein. Also giebt dann *kein* anderes Factorenpaar von *z dieselben x,* und es giebt für ein *ungerades* Factorenpaar $\varkappa$ und λ von *z nur ein* Werthenpaar von *x* (*Q.*), also für jedes *andere* $\varkappa$ und λ *andere x.* Dieses behauptet (VIII. *b.*).

b. Sind $\varkappa$ und λ zwar *theilerfremd,* aber nicht beide *ungerade,* sondern nur eins von ihnen ist es, das andere *gerade,* so sind $\frac{1}{2}\varkappa$ und 2λ *ganze* Zahlen, wenn $\varkappa$ *gerade* ist, und $2\varkappa$ und $\frac{1}{2}\lambda$ sind es, wenn λ *gerade* ist. Also giebt dann nach (139. und 140.), aufser $\sigma = \varkappa$ und $\tau = \lambda$, im *ersten* Fall auch $\sigma = \frac{1}{2}\varkappa$ und $\tau = 2\lambda$ und im *zweiten* Fall auch $\sigma = 2\varkappa$ und $\tau = \frac{1}{2}\lambda$ *dieselben x,* und folglich giebt es dann in dem einen und dem andern Fall ein *zweites* Factorenpaar $\frac{1}{2}\varkappa$ und 2λ oder $2\varkappa$ und $\frac{1}{2}\lambda$ von *z,* welchem *dieselben x* zukommen, wie den Factorenpaaren $\varkappa$ und λ selbst. Hier giebt es nun weiter zwei Fälle.

α. Ist nemlich von den *theilerfremden* $\varkappa$ und λ, $\varkappa$ zwar *gerade,* aber *nur* durch die *erste* Potenz von 2 theilbar, während, wie in (*b.*), λ *ungerade* ist, so ist umgekehrt $\frac{1}{2}\varkappa$ *ungerade* und 2λ *gerade:* also kommt dann das *zweite* Factorenpaar $\frac{1}{2}\varkappa$ und 2λ, welches nach (*b.*) *dieselben x* giebt, wie $\varkappa$ und λ selbst, unter den verschiedenen Paaren theilerfremder Factoren von *z* selbst vor, da einer mit 2^1 aufgeht, während der andere ungerade ist. Eben so verhält es sich, wenn $\varkappa$ *ungerade* und λ mit 2^1 theilbar ist. In diesem Fall also kommt jedes Werthenpaar von *x,* welches zu dieser Art von Factorenpaaren von *z* gehört, *zweimal* vor; gemäfs (VIII. *c.*).

β. Ist dagegen von den *theilerfremden* $\varkappa$ und λ, $\varkappa$ durch eine *höhere* als die erste Potenz von 2 theilbar, während λ *ungerade* ist, so sind

$\frac{1}{2}\varkappa$ und 2λ *beide gerade*. Also kommt dann das *zweite* Factorenpaar $\frac{1}{2}\varkappa$ und 2λ, welches nach (*b.*) *dieselben* x giebt wie $\varkappa$ und λ selbst, unter *denjenigen* Paaren von Factoren vor, die beide mit 2 theilbar sind. Eins der beiden Werthenpaare von x, welche Factorenpaaren *dieser* Art nach (*R.*) zukommen, ist also dann das hier zu $\varkappa$ und λ gehörige Werthenpaar von x. Eben so verhält es sich, wenn $\varkappa$ ungerade ist und λ mit einer höhern als der ersten Potenz von 2 aufgeht; gemäfs (VIII. *d.*).

c. Sind die Factoren $\varkappa$ und λ *nicht theilerfremd*, sondern mit 2 *gemeintheilbar*, so kann der eine von den beiden, z. B. $\varkappa$, nur mit der *ersten* Potenz von 2 aufgehen, wenn auch der andere mit einer höhern Potenz von 2 aufgeht, indem $\varkappa$ und λ keinen *gröfsern Gemeintheiler* als 2 haben können: also ist dann $\frac{1}{2}\varkappa$ ungerade und 2λ gerade und $\frac{1}{2}\varkappa$ und 2λ sind *theilerfremd*. Alsdann giebt es dann zwar nach (*T. i.*) *kein* anderes Factorenpaar σ und τ von z, welches dieselben *beiden* Werthenpaare von x gäbe, wie $\varkappa$ und λ, aber umgekehrt ist das zweite Werthenpaar von x, welches nach (*c. β.*) für die hier *theilerfremden* $\frac{1}{2}\varkappa$ und 2λ Statt findet, wie dort bemerkt, unter den Werthenpaaren von x enthalten, die den durch 2 gemeintheilbaren $\varkappa$ und λ zukommen. Eben so verhält es sich, wenn λ nur mit der ersten Potenz von 2 aufgeht, während vielleicht $\varkappa$ mit einer höhern als der ersten Potenz von 2 theilbar ist.

So folgt denn, dafs unter den Werthen von x, welche Factorenpaaren $\varkappa$ und λ zukommen, die mit 2 gemeintheilbar sind, zugleich diejenigen mit vorkommen, welche den *theilerfremden* Factorenpaaren entsprechen, deren einer gerade, der andere *ungerade* ist; gemäfs (VIII. *e.*).

V. a. Der erste Fall (*U. a.*) findet *ausschliefslich* Statt, wenn z *selbst* nicht mit 2 aufgeht, und also *ungerade* ist. Denn dann sind in allen theilerfremden Factorenpaaren von z *beide* Factoren *ungerade*. Es giebt alsdann *gar keine* Factoren, die mit 2 aufgehen. Also giebt es dann so viele verschiedene Werthenpaare x und $z-x$ von x, als verschiedene theilerfremde Factorenpaare von z; und diese Werthe von x sind *alle*, welche der Gleichung $x^2 = \mathfrak{G}z + 1$ genugthun; gemäfs (IX. *a.*).

b. Geht z nur mit der *ersten* Potenz von 2 auf, so giebt es weder Paare von Factoren, die *beide* ungerade sind, wie in (*a.*), noch durch 2 gemeintheilbare Factorenpaare, mithin *nur* Paare von Factoren, deren einer mit 2^1 aufgeht, der andere mit 2 gar nicht; also nur Factorenpaare von der Art wie in (*U. b. α.*). Diese Factorenpaare geben dann also auch, da es keine

andern giebt, *alle* die verschiedenen Werthenpaare x und $z-x$ von x, welche der Gleichung $x^2 = \mathfrak{S}z+1$ genugthun; und zwar giebt schon *die Hälfte* dieser Factorenpaare *alle* Werthenpaare von x, weil nach (*U. b. α.*) jedes Werthenpaar von x *zweimal* vorkommt; gemäfs (IX. *b.*).

c. Geht z mit einer *höhern* als der ersten Potenz von 2 auf, so giebt es aufser den Factorenpaaren, die 2 zum Gemeintheiler haben, zwar Paare theilerfremder Factoren von z, von welchen nur der eine mit 2 aufgeht, während der andere ungerade ist: aber die zu diesen letzten gehörigen Werthenpaare von x sind nach (*U. c.*) unter denen mitbegriffen, welche zu den mit 2 gemeintheilbaren Factorenpaaren gehören. Und da nun Paare von Factoren, die *beide ungerade* sind, in dem gegenwärtigen Falle gar nicht vorkommen, so sind hier die *Doppelpaare* der Werthe von x, welche den mit 2 gemeintheilbaren Factorenpaaren von z zukommen, *allein alle* diejenigen, welche der Gleichung $x^2 = \mathfrak{S}z+1$ genugthun; gemäfs (IX. *c.*).

Anm. *W.* Der Beweis von (VIII. und IX.) beruht insbesondere auf der Zerlegung von $\mathfrak{S}z = \mathfrak{S}\varkappa\lambda$ für die Gleichung $x^2 = \mathfrak{S}z+1$ in die beiden Factoren $\varkappa\lambda_1$ und $\lambda\varkappa_1$, wenn $\mathfrak{S} = \varkappa_1\lambda_1$ gesetzt wird; deren einer dann $= x+1$, der andere $= x-1$ ist (*N.*). Dieses giebt aus den Gleichungen (100. und 107.) die Werthe von $\varkappa_1$ und λ, und durch sie, vermöge der Gleichungen (101. und 108.), die Werthe von x. Die Untersuchung, ob mehrere Factorenpaare $\varkappa$ und λ von z *dieselben* x geben können, geschieht insbesondere dadurch, dafs man in (*T. b.*) die *gröfsten Gemeintheiler* von $\varkappa$ und σ, und λ und τ in Rechnung bringt.

§. 95.

Lehrsatz.

Man setze für eine beliebige ganze Zahl* z, *die immer durch

$$1.\quad z = 2^m . p_1^{e_1}\, p_2^{e_2}\, p_3^{e_3} \ldots . p_\mu^{e_\mu}$$

ausgedrückt werden kann, wo die* μ *verschiedenen* p *sämmtlich Stammzahlen* > 2 *sind, indem für den Fall, wo* z *den Stammtheiler* 2 *nicht enthält, nur* $m = 0$ *gesetzt werden darf,

$$2.\quad z = \varkappa\lambda.$$

Ferner bezeichne man von den verschiedenen Factorenpaaren* $\varkappa$ *und* λ, *in welche* z *sich zerlegen läfst, die Anzahl

3.
1. *Derjenigen, welche theilerfremd sind und 2 gar nicht enthalten, durch* τ_1;
2. *Derjenigen, welche theilerfremd sind, deren einer aber* 2^1 *zum Factor hat, durch* τ_2;
3. *Derjenigen, welche theilerfremd sind und deren einer eine beliebige Potenz von* 2, *höher als die erste, zum Factor hat, durch* τ_3;
4. *Derjenigen, deren gröſster Gemeintheiler* 2 *ist, durch* τ_4.

Alsdann sind die Werthe von τ_1, τ_2, τ_3 und τ_4 *in den verschiedenen Fällen, welche für* z (1.) *vorkommen können, folgende:*

Für $m>2$, *für* $m=2$, *für* $m=1$ *und für* $m=0$ *ist*

$$4.\quad\begin{cases} 1.\ \tau_1 = 0 = 0 = 0 = 2^{\mu-1}, \\ 2.\ \tau_2 = 0 = 0 = 2^{\mu} = 0, \\ 3.\ \tau_3 = 2^{\mu} = 2^{\mu} = 0 = 0, \\ 4.\ \tau_4 = 2^{\mu} = 2^{\mu-1} = 0 = 0. \end{cases}$$

Beispiele. 1. Es sei

$$5.\quad z = 240 = 2^4.3.5, \text{ wo also } m = 4 > 2,\ \mu = 2 \text{ ist.}$$

Die *sämmtlichen* Factorenpaare von z sind folgende:

$$6.\quad\begin{cases} \varkappa = 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 8\ \ 10\ \ 12\ \ 15, \\ \lambda = 240\ \ 120\ \ 80\ \ 60\ \ 48\ \ 40\ \ 30\ \ 24\ \ 20\ \ 16. \end{cases}$$

Factoren $\varkappa$ und λ von der *ersten* und *zweiten* Art (3.) kommen hier *nicht* vor; also ist $\tau_1=0$ und $\tau_2=0$. Factorenpaare der *dritten* Art sind die vier 1, 240; 3, 80; 5, 48 und 15, 16; also ist hier $\tau_3=4=2^{\mu}$; gemäſs (4. 3.). Factorenpaare der *vierten* Art sind die vier 2, 120; 6, 40; 8, 30 und 10, 24; also ist $\tau_4=4=2^{\mu}$; gemäſs (4. 4.). Die beiden noch übrigen Factorenpaare 4, 60 und 12, 20 kommen nicht in Betracht, da sie $4>2$ zum Gemeintheiler haben.

2. Es sei

$$7.\quad z = 420 = 2^2.3.5.7, \text{ wo also } m = 2,\ \mu = 3 \text{ ist.}$$

Die *sämmtlichen* Factorenpaare von z sind folgende:

$$8.\quad\begin{cases} \varkappa = 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 10\ \ 12\ \ 14\ \ 15\ \ 20, \\ \lambda = 420\ \ 210\ \ 140\ \ 105\ \ 84\ \ 70\ \ 60\ \ 42\ \ 35\ \ 30\ \ 28\ \ 21. \end{cases}$$

Factorenpaare $\varkappa$ und λ von der *ersten* und *zweiten* Art (3.) kommen wieder nicht vor; also ist $\tau_1=0$ und $\tau_2=0$. Von der dritten Art (3.) sind die acht 1, 420; 3, 140; 4, 105; 5, 84; 7, 60; 12, 35; 15, 28 und 20, 21; also ist $\tau_3=8=2^{\mu}$; gemäſs (4. 3.). Von der vierten Art sind die vier 2, 210; 6, 70; 10, 42 und 14, 30, also ist $\tau_4=4=2^{\mu-1}$; gemäſs (4. 4.).

3. Es sei

9. $z=630=2.3^2.5.7$, wo also $m=1$, $\mu=3$ ist.

Die *sämmtlichen* Factorenpaare von z sind folgende:

$$10. \begin{cases} \varkappa = & 1\ \ 2\ \ 3\ \ 5\ \ 6\ \ 7\ \ 9\ 10\ 14\ 15\ 18\ 21, \\ \lambda = & 630\ 315\ 210\ 126\ 105\ 90\ 70\ 63\ 45\ 42\ 35\ 30. \end{cases}$$

Factorenpaare $\varkappa$ und λ von der *ersten* Art (3.) kommen nicht vor; also ist $\tau_1=0$. Von der *zweiten* Art sind die acht 1, 630; 2, 315; 5, 126; 7, 90; 9, 70; 10, 63; 14, 45 und 18, 35, also ist $\tau_2=8=2^\mu$; gemäfs (4. 2.). Factorenpaare der *dritten* und *vierten* Art kommen nicht vor; also ist $\tau_3=0$ und $\tau_4=0$. Die vier übrigen Factorenpaare 3, 210; 6, 105; 15, 42 und 21, 30 kommen nicht in Betracht, da sie *gröfsere* Gemeintheiler als 2 haben.

4. Es sei

11. $z=1575=3^2.5^2.7$, wo also $m=0$ und $\mu=3$ ist.

Die *sämmtlichen* Factorenpaare von z sind folgende:

$$12. \begin{cases} \varkappa = & 1\ \ 3\ \ 5\ \ 7\ \ 9\ \ 15\ 21\ 25\ 35, \\ \lambda = & 1575\ 525\ 315\ 225\ 175\ 105\ 75\ 63\ 45. \end{cases}$$

Factorenpaare der ersten Art sind die vier 1, 1575; 7, 225; 9, 175; 25, 63, also ist $\tau_1=4=2^{\mu-1}$; gemäfs (4. 1.). Von der 2ten, 3ten und 4ten Art kommen keine Factoren vor, also ist $\tau_2=0$, $\tau_3=0$, $\tau_4=0$. Die noch übrigen Factorenpaare haben gröfsere Zahlen als 2 zu Gemeintheilern.

Beweis. *A.* Da von z nur diejenigen Factorenpaare $\varkappa$ und λ gesucht werden, die entweder theilerfremd sind, oder die keinen gröfsern Gemeintheiler als 2 haben, so kommt es auf alle die, welche irgend eines der $p>2$ *in $\varkappa$ und λ zugleich* enthalten, gar nicht an. Es darf also keine Potenz irgend eines p *zerfället* werden, sondern immer nur die *volle* Potenz in $\varkappa$ oder in λ vorkommen. Man kann also in (1.)

13. $p_1^{e_1}=P_1$, $p_2^{e_2}=P_2$, $p_3^{e_3}=P_3$, ... $p_\mu^{e_\mu}=P_\mu$,

und folglich

14. $z=2^m.P_1.P_2.P_3....P_\mu$

setzen und hierin die P als *untheilbare* Zahlen betrachten.

B. Gesetzt nun, es wäre zuerst $m=0$, also blofs

15. $z=P_1.P_2.P_3....P_\mu$,

so kann man zuerst $\varkappa=1$ und λ gleich dem Product *aller* P setzen; sodann $\varkappa$ gleich *jedem* der μ verschiedenen P; λ gleich dem Product der $\mu-1$ übrigen. Ferner $\varkappa$ gleich dem Product jeder *zwei* P; λ gleich dem Product der

$\mu-2$ übrigen. Weiter $\varkappa$ gleich dem Product jeder ***drei P;*** λ gleich dem Product der $\mu-3$ übrigen u. s. w.

Daraus folgt, dafs die Anzahl der verschiedenen Werthe, welche $\varkappa$ haben kann, keine andere ist, als die Anzahl aller möglichen Producte von einem, zwei, drei bis μ verschiedenen P; wozu auch noch 1 kommt. Diese verschiedenen Producte enthält nach (§. 2.) das Product

$$16.\quad (1+P_1)(1+P_2)(1+P_3)\dots(1+P_\mu)$$

sämmtlich, und ihre Anzahl ist nach (§. 3.) $=2^\mu$.

Aber offenbar kommen auf diese Weise die verschiedenen möglichen Factorenpaare jedes *zweimal* vor. Denn wegen $z=\varkappa\lambda$ ist $\lambda=\frac{z}{\varkappa}$, und $\frac{z}{\varkappa}$ ist ebensowohl ein Theiler von z, also ebensowohl ein $\varkappa$, als $\varkappa$ selbst. Die λ sind nichts anderes als die sämmtlichen $\varkappa$ selbst, aber in umgekehrter Ordnung. Der ***verschiedenen*** Factorenpaare giebt es also nur $\frac{1}{2}.2^\mu=2^{\mu-1}$ und daher ist

$$17.\quad \tau_1=2^{\mu-1} \text{ für } m=0:$$

denn die τ_1 Factorenpaare sind es in (3.), welche, wie hier, den Theiler 2 *gar nicht* haben sollen; gemäfs (4.).

Factoren, welche 2 enthalten, wie (3. 2., 3. und 4.) giebt es hier gar nicht; also ist

$$18.\quad \tau_2=0,\quad \tau_3=0,\quad \tau_4=0 \quad \text{für} \quad m=0;$$

gemäfs (4.).

C. Gesetzt es sei weiter in (14.) m nicht $=0$, sondern $m=1$, also

$$19.\quad z=2P_1.P_2.P_3\dots P_\mu,$$

so kommen *nur* Factorenpaare der *zweiten* Art (3.) vor; denn *alle* haben nothwendig den Theiler 2^1, der sich immer entweder in $\varkappa$ oder in λ befinden mufs.

Man bezeichne die verschiedenen möglichen Producte von einem, zwei, drei etc. P zusammengenommen durch $\overset{1}{P}, \overset{2}{P}, \overset{3}{P}, \dots \overset{\mu}{P}$ und bringe den Theiler 2 ausschliefslich in die $\varkappa$, so werden durch

$$20.\quad \begin{cases} \varkappa = 2,\ 2(\overset{1}{P}),\ 2(\overset{2}{P}),\ 2(\overset{3}{P}),\ \dots\ 2(\overset{\mu}{P}) \text{ und} \\ \lambda = (\overset{\mu}{P}),\ (\overset{\mu-1}{P}),\ (\overset{\mu-2}{P}),\ (\overset{\mu-3}{P}),\ \dots\ 1 \end{cases}$$

sämmtliche Factorenpaare von z ausgedrückt. Aber *alle* $\varkappa$ sind hier von den λ *verschieden:* denn alle $\varkappa$ gehen mit 2 auf, alle λ nicht. Die Anzahl der Factorenpaare τ_2 ist also die der $\varkappa$ in (20.) selbst, und diese ist gemäfs (***B.***) $=2^\mu$. Also ist hier

21. $\tau_2 = 2^\mu$ und $\tau_1 = 0$, $\tau_3 = 0$, $\tau_4 = 0$; für $m = 1$; gemäfs (4.).

D. Es sei in (14.) $m = 2$, also

$$22. \quad z = 2^2 . P_1 . P_2 . P_3 \ldots . P_\mu .$$

Factorenpaare der *ersten* und *zweiten* Art (3.) kommen hier nicht vor, denn kein Factorenpaar ist *ohne* den Theiler 2; wenn 2 in dem einen Factor *nicht* vorkommt, so kommt in dem andern nicht blofs 2^1, sondern 2^2 vor. Also giebt es hier nur Factorenpaare der *dritten* und *vierten* Art (3.).

Die von der *dritten* Art sind diejenigen, deren einer 2 gar nicht, der andere 2^2 enthält. Sie werden also ganz auf dieselbe Weise ausgedrückt, wie die in (20.), wenn man daselbst 2^2 statt 2 schreibt. Ihre Anzahl τ_3 ist also, wie die der dortigen, $= 2^\mu$.

Die Factorenpaare der *vierten* Art sind hier diejenigen $\varkappa$ und λ, welche *jeder* 2 zum Theiler haben. Sie werden also nach der Bezeichnungsart von (*C.*) durch

$$23. \quad \begin{cases} \varkappa = \quad 2, \quad 2(\overset{1}{P}), \; 2(\overset{2}{P}), \; 2(\overset{3}{P}), \ldots . \; 2(\overset{\mu}{P}), \\ \lambda = 2(\overset{\mu}{P}), \; 2(\overset{\mu-1}{P}), \; 2(\overset{\mu-2}{P}), \; 2(\overset{\mu-3}{P}), \ldots . \quad 2 \end{cases}$$

ausgedrückt. Hier sind offenbar wieder die sämmtlichen λ den $\varkappa$ in umgekehrter Ordnung gleich, wie in dem Fall in (*B.*). Also ist die Anzahl τ_4 der von einander *verschiedenen* Factorenpaare nur, wie dort, $= 2^{\mu-1}$.

Mithin ist zusammengenommen

24. $\tau_3 = 2^\mu$, $\tau_4 = 2^{\mu-1}$, $\tau_1 = 0$, $\tau_2 = 0$ für $m = 2$; gemäfs (4.).

E. Es sei endlich in (14.) $m > 2$.

Auch hier kommen Factorenpaare der *ersten* und *zweiten* Art (3.) nicht vor; denn kein Factorenpaar ist *ohne* den Theiler 2; und kommt 2 in dem einen Factor *nicht* vor, so kommt in dem andern nicht blofs 2^1, sondern 2^m vor. Also giebt es auch hier wieder nur Factorenpaare der *dritten* und *vierten* Art (3.).

Die von der *dritten* Art sind diejenigen, deren einer 2 gar nicht, der andere 2^m enthält. Sie werden also wieder ganz auf dieselbe Weise ausgedrückt wie die in (20.), wenn man daselbst 2^m statt 2 schreibt. Ihre Anzahl τ_3 ist daher, wie die der dortigen, $= 2^\mu$.

Die Factorenpaare der *vierten* Art sind hier diejenigen $\varkappa$ und λ, deren einer 2, der andere 2^{m-1} zum Theiler haben. Sie werden also nach der Be-

zeichnungsart von (*C.*) durch

$$25.\quad \begin{cases} \varkappa = 2, & 2(\overset{1}{P}), \quad 2(\overset{2}{P}), \quad 2(\overset{3}{P}), \quad \ldots \; 2(\overset{\mu}{P}), \\ \lambda = 2^{m-1}(\overset{\mu}{P}), & 2^{m-1}(\overset{\mu-1}{P}), \quad 2^{m-1}(\overset{\mu-2}{P}), \quad 2^{m-1}(\overset{\mu-3}{P}), \quad \ldots \; 2^{m-1} \end{cases}$$

ausgedrückt. Hier sind offenbar die sämmtlichen λ von den $\varkappa$ *verschieden*, wie in dem Fall (*C.*). Also ist die Anzahl τ_4 der Factorenpaare der vierten Art, wie dort, $= 2^\mu$.

Mithin ist zusammengenommen

$$26.\quad \tau_3 = 2^\mu,\ \tau_4 = 2^\mu,\ \tau_1 = 0,\ \tau_2 = 0 \text{ für } m > 2;$$

gemäfs (4.).

§. 96.

Lehrsatz.

Es sei z *eine beliebige ganze Zahl, die, wie in* (§. 95.), *immer durch*

$$1.\quad z = 2^m \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_\mu^{e_\mu}$$

ausgedrückt werden kann, wo die μ *verschiedenen* p *sämmtlich Stammzahlen* > 2 *sind. Alsdann ist in der Gleichung*

$$2.\quad x^2 = \mathfrak{S}z + r,$$

wo x *und* r *zu* z *theilerfremd und* $<$ z *sind, die Anzahl* n *der Paare zu* z *theilerfremder Werthe von* x, *die zu einem und demselben* r *gehören, also die Anzahl der Quadratwurzelpaare zu* r, *für jedes* r *gleichmäfsig, also auch für* r $= 1$:

$$3.\quad n = 2^{\mu-1} \text{ für } m = 0,$$

$$4.\quad n = 2^{\mu-1} \text{ für } m = 1,$$

$$5.\quad n = 2^{\mu} \text{ für } m = 2,$$

$$6.\quad n = 2^{\mu+1} \text{ für } m > 2.$$

Dagegen die Anzahl ν *der in* (2.) *möglichen verschiedenen* r $<$ z, *also die Anzahl der Quadratreste zu* z *ist, wenn, wie immer,* φz *die Anzahl der zu* z *theilerfremden Zahlen* > 0 *und* $<$ z *bezeichnet,*

$$7.\quad \nu = \frac{\varphi z}{2n};$$

wo n, *nach den verschiedenen Werthen von* m *in* (1.), *die Werthe* (3. 4. 5. 6.) *hat und nach* (§. 81. 7.)

$$8.\quad \varphi z = 2^{m-1} \cdot p_1^{e_1-1} \cdot p_2^{e_2-1} \cdots p_\mu^{e_\mu-1} (p_1-1)(p_2-1)\ldots(p_\mu-1)$$

ist, so dafs also φz *und* 2n, *folglich auch* ν, *unmittelbar aus der gegebenen Zahl* z (1.) *gefunden werden kann.*

Beispiel 1. Die Zahl $z=45$ in dem *zweiten* Beispiel zu (§. 94.) ist

9. $z = 45 = 3^2.5;$

also ist für sie, mit (1.) verglichen,

10. $m=0, \quad \mu=2.$

Nach (§. 94. 47.) giebt es zu jedem der $\nu=6$ verschiedenen Werthe, welche r haben kann, $n=2$ *Werthenpaare* von x, und φz ist nach (8.) $=3^{2-1}(3-1)(5-1)=3.2.4=24$. Zufolge (3.) ist $n=2^{\mu-1}=2$ und zufolge (6.) $\nu=\frac{24}{2.2}=6$; wie gehörig.

2. Die Zahl $z=126$ in dem *dritten* Beispiel zu (§. 94.) ist

11. $z = 126 = 2.3^2.7;$

also ist für sie, mit (1.) verglichen,

12. $m=1, \quad \mu=2.$

Nach (§. 94. 55.) giebt es für jeden der $\nu=9$ verschiedenen Werthe von r $n=2$ *Werthenpaare* von x, und φz ist nach (8.) $=1.3^{2-1}(3-1)(7-1)=3.2.6=36$. Zufolge (3.) ist $n=2^{\mu-1}=2$ und zufolge (6.) $\nu=\frac{36}{2.2}=9$; wie gehörig.

3. Die Zahl $z=180$ in dem *ersten* Beispiel zu (§. 94.) ist

13. $z=180=2^2.3^2.5;$

also ist hier, mit (1.) verglichen,

14. $m=2$ und $\mu=2.$

Nach (§. 94. 25.) gehören zu jedem der $\nu=6$ verschiedenen Werthe von r $n=4$ *Werthenpaare* von x, und φz ist nach (8.) $=2.3^{2-1}(3-1)(5-1)=2.3.2.4=48$. Zufolge (3.) ist $n=2^{\mu}=4$ und zufolge (6.) $r=\frac{48}{2.4}=6$; wie gehörig.

4. Die Zahl $z=120$ in dem *vierten* Beispiele zu (§. 94.) ist

15. $z=120=2^3.3.5;$

also ist für sie, mit (1.) verglichen,

16. $m=3>2$ und $\mu=2.$

Nach (§. 91. 62. und 67.) gehören zu jedem der $\nu=2$ verschiedenen Werthe von r, $n=8$ Werthenpaare von x, und φz ist nach (8.) $=2^2(3-1)(5-1)=4.2.4=32$. Zufolge (6.) ist $n=2^{\mu+1}=8$ und zufolge (7.) $r=\frac{32}{2.8}=2$; wie gehörig.

Beweis. *A.* Zunächst ist zu bemerken, dafs nach (§. 94. II.) zu *jedem* Werth von r in (2.) *gleichviele* x gehören, also eben so viele, als zu $r=1$. Es kommt also nur auf den Fall $r=1$ an.

B. Ist nun *Erstlich* $m=0$, so ist z *ungerade* und befindet sich also in dem Fall (§. 94. IX. *a.*). In diesem Fall ist nach (§. 94. IX. *a.*) die Anzahl n der Werthenpaare von x, welche der Gleichung

$$17. \quad x^2 = \mathfrak{G}z+1$$

genugthun, der Anzahl der *theilerfremden* Factorenpaare von z gleich. Diese Anzahl ist nach (§. 95. 4. 1.) $\tau_1 = 2^{\mu-1}$, also ist $n=2^{\mu-1}$; gemäfs (3.).

C. Ist *Zweitens* $m=1$, so geht z nur mit 2^1 auf und ist also in dem Falle (§. 94. IX. *b.*). In diesem Fall giebt es nach (§. 94. IX. *b.*) *halb* so viele Werthenpaare von x, welche der Gleichung (17.) genugthun, als *theilerfremde* Factorenpaare von z, von welchen allen je einer 2^1 zum Factor hat. Die Anzahl *dieser* theilerfremden Factorenpaare ist nach (§. 95. 4. 2.) $\tau_2 = 2^\mu$, also ist hier $n=\frac{1}{2}.2^\mu = 2^{\mu-1}$; gemäfs (4.).

D. Ist *Drittens* $m=2$, so geht z mit einer *höhern* als der ersten Potenz von 2 auf und ist also in dem Falle (§. 94. IX. *c.*). In diesem Fall giebt es nach (§. 94. IX. *c.*) *doppelt* so viele Werthenpaare von x, welche der Gleichung (16.) genugthun, als Factorenpaare von z, die 2 zum *gröfsten* Gemeintheiler haben. Die Anzahl *dieser* Factorenpaare ist diejenige τ_4 in (§. 95. 3. 4.), und nach (§. 95. 4. 4.) ist für $m=2$, $\tau_4 = 2^{\mu-1}$; also ist hier $n=2.2^{\mu-1}=2^\mu$; gemäfs (5.).

E. Ist endlich *Viertens* $m>2$, so verhält sich zwar zunächst Alles wie in (*D.*), aber τ_4 ist in diesem Fall nach (§. 95. 4. 4.) $=2^\mu$: also ist hier $m=2.2^\mu = 2^{\mu+1}$; gemäfs (6.).

F. Die Gleichung (7.) im Lehrsatze folgt unmittelbar aus (§. 94. 4.).

Anm. *G.* Wenn z eine einfache ungerade Stammzahl p ist, so ist in (1.) $m=0$ und $\mu=1$. Also ist in diesem Fall nach (3. und 7.)

$$18. \quad n=1,$$

mithin giebt es *nur ein* Werthenpaar x und $z-x$ zu jedem der Quadratreste r. Ferner sind hier alle $p-1$ Zahlen 1, 2, 3, 4, ... $p-1$ zu $z=p$ theilerfremd, also ist $\varphi z = p-1$; und dies giebt nach (7.) und (17.)

$$19. \quad \nu = \tfrac{1}{2}(p-1).$$

Die Anzahl ν der verschiedenen Quadratreste zu p ist also $\frac{1}{2}(p-1)$: alles wie es nach (§. 45.) sein mufs.

§. 97.

Erklärung.

I. *Wenn in der Gleichung*

$$1. \quad z = p^e$$

p *eine beliebige ungerade Stammzahl, also* >2, e *eine beliebige positive ganze Zahl ist, und die zu den Zahlen* z_φ, *welche* >0 *und* $<z$ *und zu* z *theilerfremd sind, gehörigen Quadratreste durch* r, *die Nichtquadratreste durch* w *bezeichnet werden, so dafs also etwa*

$$2.\quad x^2 = \mathfrak{G}z + r \text{ und}$$
$$3.\quad uv = \mathfrak{G}z + w$$

gesetzt wird, wo nun x, u, v, r *und* w *sämmtlich aus den zu* z *theilerfremden Zahlen* $z_\varphi > 0$ *und* $<z$ *genommen sind: so ist die Anzahl der verschiedenen* r, *welche Statt finden, der Anzahl der verschiedenen möglichen* w *gleich, und jede ist* $=\frac{1}{2}\varphi z$, *wo* φz *wie immer die Anzahl der Zahlen* z_φ *bezeichnet; so dafs also die Hälfte der zu* z *theilerfremden* φz *Zahlen* $z_\varphi > 0$ *und* $<z$ *Quadratreste, die andere Hälfte Nichtquadratreste zu den Zahlen* z_φ *selbst sind.*

Desgleichen ist für $z=p^e$ (1.), r *und* w *mögen kleiner oder gröfser als* z *sein,*

$$4.\quad r^{\frac{1}{2}\varphi z} = \mathfrak{G}z+1 \text{ für jeden Quadratrest } r,$$
$$5.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}z-1 \text{ für jeden Nichtquadratrest } w.$$

Allgemein ist für jede beliebige, zu $z=p^e$ *theilerfremde positive Zahl* z_φ, *sie mag kleiner oder gröfser als* z *sein,*

$$6.\quad z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z \pm 1 \text{ für } z=p^e \text{ (1.)}.$$

II. *Jeder Nichtquadratrest* w *zu* p *ist zugleich Nichtquadratrest zu* $z=p^e$ *für ein beliebiges ganzes positives* e; *und umgekehrt.*

Und wenn die ungerade Stammzahl p *eine der Stammfactoren einer beliebigen Zahl* Z *ist, so giebt es immer zu* Z *theilerfremde Zahlen* $W>0$ *und* $<Z$, *die zu* p *und zu* Z, *also auch zu* p^e *und zu* Z *zugleich Nichtquadratreste sind. Sie werden, wenn man das Product der ersten Potenzen aller der Stammfactoren, die* Z *noch aufser* p *hat, durch* P *bezeichnet, durch*

$$7.\quad W = n_1 p + w \text{ und}$$
$$8.\quad W = n_2 P + 1$$

zugleich ausgedrückt, wo $n_1 > 0$ *und* $<P$ *und* $n_2 > 0$ *und* $<p$ *ist.*

Beispiel zu I. Es sei

$$9.\quad z = 3^4 = 81,\ \text{also}\ p=3,\ e=4,$$

so sind die zu z theilerfremden Zahlen z_φ und die dazu gehörigen *Quadratreste r* folgende:

$$10.\ \begin{cases} z_\varphi = \overset{*}{1}\ 2\ \overset{*}{4}\ 5\ \overset{*}{7}\ 8\ \overset{*}{10}\ 11\ \overset{*}{13}\ 14\ \overset{*}{16}\ 17\ \overset{*}{19}\ 20\ \overset{*}{22}\ 23\ \overset{*}{25}\ 26\ \overset{*}{28}\ 29\ \overset{*}{31}\ 32\ \overset{*}{34}\ 35\ \overset{*}{37}\ 38\ \overset{*}{40} \\ r = 1\ 4\ 16\ 25\ 49\ 64\ 19\ 40\ 7\ 34\ 13\ 46\ 37\ 76\ 79\ 43\ 58\ 28\ 55\ 31\ 70\ 52\ 22\ 10\ 73\ 67\ 61 \\ z_\varphi = 41\ \overset{*}{43}\ 44\ \overset{*}{46}\ 47\ \overset{*}{49}\ 50\ \overset{*}{52}\ 53\ \overset{*}{55}\ 56\ \overset{*}{58}\ 59\ \overset{*}{61}\ 62\ \overset{*}{64}\ 65\ \overset{*}{67}\ 68\ \overset{*}{70}\ 71\ \overset{*}{73}\ 74\ \overset{*}{76}\ 77\ \overset{*}{79}\ 80 \\ r = 61\ 67\ 73\ 10\ 22\ 52\ 70\ 31\ 55\ 28\ 58\ 43\ 79\ 76\ 37\ 46\ 13\ 34\ 7\ 40\ 19\ 64\ 49\ 25\ 16\ 4\ 1. \end{cases}$$

Die Anzahl φz der Zahlen z_φ ist hier $\varphi z = 54$. Die Anzahl der verschiedenen ***Quadratreste*** r ist, wie sich zeigt, $= 27$. Es sind die mit einem Sternchen bezeichneten z_φ. Die übrigen 27 Zahlen z_φ sind daher ***Nichtquadratreste*** w. Also sind die ***Hälfte*** der Zahlen z_φ Quadratreste, die andere ***Hälfte*** Nichtquadratreste.

Ferner soll nach dem Lehrsatze (4. und 5.), da hier $\varphi z = 27$ ist, für jeden ***Quadratrest*** r, $r^{27} = \mathfrak{G}.81 + 1$, und für jeden ***Nichtquadratrest*** w, $w^{27} = \mathfrak{G}.81 - 1$ sein. In der That giebt z. B. $r = 19$, $19^3 = 6859 = \mathfrak{G}.81 + 55$, also $19^9 = (\mathfrak{G}.81 + 55)^3 = \mathfrak{G}.81 + 166375 = \mathfrak{G}.81 + 1$ und $19^{27} = (\mathfrak{G}.81 + 1)^3 = \mathfrak{G}.81 + 1$; wie es sein soll. $w = 17$ giebt $17^3 = 4913 = \mathfrak{G}.81 + 53$, also $17^9 = (\mathfrak{G}.81 + 53)^3 = \mathfrak{G}.81 + 148877 = \mathfrak{G}.81 - 1$, und folglich $17^{27} = (\mathfrak{G}.81 - 1)^3 = \mathfrak{G}.81 - 1$; ebenfalls wie es sein soll.

Beispiel zu II. *a.* Es sei

$$11.\quad p = 3,\quad p^e = 3^4 = 81.$$

Der einzige ***Nichtquadratrest*** zu p ist $w = 2$; denn es ist für die beiden zu 3 theilerfremden Zahlen 1 und 2 $1^2 = \mathfrak{G}3 + 1$ und $2^2 = \mathfrak{G}3 + 1$. Dieses $w = 2$ ist, wie aus (10.) zu sehen, auch Nichtquadratrest zu $p^e = 81$. Umgekehrt sind alle die Nichtquadratreste zu $3^4 = 81$, welches die in (10.) ***nicht*** mit einem Sternchen bezeichneten Zahlen 2, 5, 8, 11, 14 u. s. w. sind, auch ***Nichtquadratreste*** zu $p = 3$, denn alle diese Zahlen werden durch $\mathfrak{G}p + 2$ ausgedrückt, und dieses ist mit $w = 2$ ***zugleich*** Nichtquadratrest zu $p = 3$.

b. Es sei

$$12.\quad p = 5,\ p^e = 5^2 = 25 \text{ und } Z = 2.3^2.5 = 90, \text{ also } P = 2.3 = 6.$$

Die zu diesen drei Zahlen theilerfremden Zahlen, kleiner als sie, sind mit ihren ***Quadratresten*** r folgende:

$$13.\ \begin{cases} 5_\varphi = \overset{*}{1}\ 2\ 3\ \overset{*}{4}, \\ r = 1\ 4\ 4\ 1; \end{cases}$$

$$14.\ \begin{cases} 25_\varphi = \overset{*}{1}\ 2\ 3\ \overset{*}{4}\ \overset{*}{6}\ 7\ 8\ \overset{*}{9}\ \overset{*}{11}\ 12\ 13\ \overset{*}{14}\ \overset{*}{16}\ 17\ 18\ \overset{*}{19}\ \overset{*}{21}\ 22\ 23\ \overset{*}{24}, \\ r = 1\ 4\ 9\ 16\ 11\ 24\ 14\ 6\ 21\ 19\ 19\ 21\ 6\ 14\ 24\ 11\ 16\ 9\ 4\ 1; \end{cases}$$

$$15.\ \begin{cases} 90_\varphi = \overset{*}{1}\ 7\ 11\ 13\ 17\ \overset{*}{19}\ 23\ 29\ \overset{*}{31}\ 37\ 41\ 43\ 47\ \overset{*}{49}\ 53\ 59\ \overset{*}{61}\ 67\ 71\ 73\ 77\ \overset{*}{79}\ 83\ 89, \\ r = 1\ 49\ 31\ 79\ 19\ 1\ 79\ 31\ 61\ 19\ 61\ 49\ 49\ 61\ 19\ 61\ 31\ 79\ 1\ 19\ 71\ 31\ 49\ 1. \end{cases}$$

Die *Nichtquadratreste* zu den drei Zahlen sind also

16. Zu $p = 5$, $w = 2\ 3$,

17. Zu $p^e = 25$, $w = 2\ 3\ 7\ 8\ 12\ 13\ 17\ 18\ 22\ 23$,

18. Zu $Z = 90$, $W = 7\ 11\ 13\ 17\ 23\ 29\ 37\ 41\ 43\ 47\ 53\ 59\ 67\ 71\ 73\ 77\ 83\ 89$.

Die Nichtquadratreste 2 und 3 (16.) sind wieder zugleich Nichtquadratreste zu $p^e = 25$ (17.); und umgekehrt können alle Nichtquadratreste zu $p^e = 25$ (17.) durch $\mathfrak{G}p + 2, 3$ ausgedrückt werden und sind also auch Nichtquadratreste zu $p = 5$.

Ferner giebt (7.), wenn man der Reihe nach $n_1 = 1, 2, 3, 4, 5$ ($< P$) und nach (16.) $w = 2$ und 3 setzt,

$$19.\quad W = \begin{cases} 7\ 12\ 17\ 22\ 27, \\ 8\ 13\ 18\ 23\ 28, \end{cases}$$

und (8.) giebt, wenn man der Reihe nach $n_2 = 1, 2, 3, 4$ ($< p$) setzt,

$$20.\quad W = 7\ 13\ 19\ 25.$$

Von diesen Werthen von W (19. und 20.) treffen $W = 7$ und 13 *zusammen*, das heifst, 7 und 13 erfüllen die beiden Gleichungen (7. und 8.) *zugleich*. Und diese beiden $W > 0$ und $< Z$ sind, wie nach (13. 14. und 15.) zu sehen, Nichtquadratreste von $p = 5$, $p^e = 25$ und $Z = 90$ *zugleich*.

Beweis von I. *A.* Man setze in (2.) der Reihe nach *die erste Hälfte* aller φz Werthe von z_φ, nemlich die $\frac{1}{2}\varphi z$ Werthe von z_φ, welche > 0 und $< \frac{1}{2}z$ sind, statt x. Die andere Hälfte der $z_\varphi > \frac{1}{2}z$ und $< z$ wird durch $z - z_\varphi$ ausgedrückt, wo $z_\varphi < \frac{1}{2}z$ ist; denn wenn z_φ keinen Theiler mit z gemein hat, so gilt das Gleiche auch von $z - z_\varphi$. Es giebt aber in (2.) $z - z_\varphi$ *denselben* Werth von r als z_φ, denn es ist

$$21.\quad (z - z_\varphi)^2 = \mathfrak{G}z + z_\varphi^2 = \mathfrak{G}z + \mathfrak{G}z + r = \mathfrak{G}z + r:$$

also kann es in (2.) *nicht mehr* als $\frac{1}{2}\varphi z$ *verschiedene* Werthe von r geben, und *alle* verschiedenen Werthe von r, welche es giebt, finden sich aus (2.) schon, wenn man dem x in (2.) die $\frac{1}{2}\varphi z$ Werthe von $z_\varphi > 0$ und $< \frac{1}{2}z$ beilegt.

B. Nun seien x_1 und x_2 zwei *beliebige* Werthe von x in (2.), beide aus den Zahlen z_φ und beide $< \frac{1}{2}z$. Gäben diese beiden Werthe von x *einen* und *denselben* Werth von r, so dafs

$$22.\quad x_1^2 = \mathfrak{G}z + r \text{ und}$$

$$23.\quad x_2^2 = \mathfrak{G}z + r$$

wäre, so müfste gemäfs (22. und 23.)

$$24.\quad x_1^2 - x_2^2 = \mathfrak{G}z \text{ oder}$$

$$25.\quad (x_1 + x_2)(x_1 - x_2) = \mathfrak{G}z = \mathfrak{G}p^e$$

sein, also müfsten entweder *Erstlich* x_1+x_2 oder x_1-x_2 mit p^e aufgehen, oder es müfsten *Zweitens* x_1+x_2 etwa mit p^n und x_1-x_2 mit p^{e-n} aufgehen, also x_1+x_2 und x_1-x_2 beide zugleich mit p, so dafs

$$26.\quad x_1+x_2=\mathfrak{G}p \text{ und}$$

$$27.\quad x_1-x_2=\mathfrak{G}p \text{ wäre.}$$

C. Mit $p^e=z$ kann *Erstlich* weder x_1+x_2 noch x_1-x_2 aufgehen, da x_1 und x_2 nach der Voraussetzung beide $<\frac{1}{2}z$ sind und also sowohl x_1+x_2 als $x_1-x_2<z$ ist.

D. Gingen *Zweitens* x_1+x_2 und x_1-x_2 beide zugleich mit p auf, so dafs also die Gleichungen (26. und 27.) Statt fänden, so müfste diesen Gleichungen zufolge, wenn man sie addirt und subtrahirt,

$$28.\quad 2x_1=\mathfrak{G}p \text{ und}$$

$$29.\quad 2x_2=\mathfrak{G}p$$

sein; also müfste, da $p>2$ vorausgesetzt wird, mithin 2 mit p nicht aufgeht, x_1 und x_2 zugleich mit p aufgehen, folglich mit $z=p^e$ den Stammtheiler $p>1$ *gemein* haben. Dieses ist der Voraussetzung entgegen, da x_1 und x_2 aus den Zahlen z_φ genommen werden sollen, die mit z *keinen* Stammtheiler >1 gemein haben. Also können in (25.) auch x_1+x_2 und x_1-x_2 nicht beide zugleich mit p aufgehen.

E. Es kann also überhaupt die Gleichung (25.), oder die (24.), also (22. und 23.) *nicht* Statt finden, das heifst: es können keine zwei $x=z_\varphi$ $<\frac{1}{2}z$ *denselben* Quadratrest r geben. Mithin sind die Quadratreste zu allen den $\frac{1}{2}\varphi z$ Zahlen $z_\varphi>0$ und $<\frac{1}{2}z$ *verschieden*, und folglich giebt es auch *nicht weniger* als $\frac{1}{2}\varphi z$ verschiedene Quadratreste zu z. Da es nun nach (*A.*) auch *nicht mehr* giebt, so ist die Anzahl der *Quadratreste* zu $z=p^e$ aus den Zahlen z_φ nothwendig *gleich* $\frac{1}{2}\varphi z$.

F. Es giebt aber φz verschiedene Zahlen z_φ. Also mufs, da die *Hälfte* davon *Quadratreste* sind, die andere *Hälfte* nothwendig *Nichtquadratreste* sein; wie es der Lehrsatz behauptet.

G. Es ist ferner nach dem allgemeinen *Fermat*schen Lehrsatze (§. 87.) für *jedes* z_φ:

$$30.\quad z_\varphi^{\varphi z}=\mathfrak{G}z+1,$$

woraus

$$z_\varphi^{\varphi z}-1=\mathfrak{G}z \text{ oder}$$

$$31.\quad (z_\varphi^{\frac{1}{2}\varphi z}+1)(z^{\frac{1}{2}\varphi z}-1)=\mathfrak{G}z$$

und hier für $z=p^e$

$$32.\quad (z_\varphi^{\frac{1}{2}\varphi z}+1)(z_\varphi^{\frac{1}{2}\varphi z}-1) = \mathfrak{G}p^e$$

folgt, so dafs also entweder *Erstlich* $z_\varphi^{\frac{1}{2}\varphi z}+1$ etwa mit p^n und $z_\varphi^{\frac{1}{2}\varphi z}-1$ mit p^{e-n}, folglich $z_\varphi^{\frac{1}{2}\varphi z}+1$ und $z_\varphi^{\frac{1}{2}\varphi z}-1$ beide mit p aufgehen müssen, dergestalt dafs die Gleichungen

$$33.\quad z_\varphi^{\frac{1}{2}\varphi z}+1 = \mathfrak{G}p \text{ und}$$

$$34.\quad z^{\frac{1}{2}\varphi z}-1 = \mathfrak{G}p$$

zugleich für *ein- und dasselbe* z_φ Statt finden, oder dafs *Zweitens entweder* $z_\varphi^{\frac{1}{2}\varphi z}+1$ *oder* $z_\varphi^{\frac{1}{2}\varphi z}-1$ mit $p^e=z$ selbst aufgehen mufs, und dafs also

$$35.\quad \text{entweder } z_\varphi^{\frac{1}{2}\varphi z}+1 = \mathfrak{G}z$$

$$36.\quad \text{oder } z_\varphi^{\frac{1}{2}\varphi z}-1 = \mathfrak{G}z$$

sein mufs.

H. Das *Erste*, dafs $z_\varphi^{\frac{1}{2}\varphi z}+1$ und $z^{\frac{1}{2}\varphi z}-1$ beide zugleich mit p aufgehen, oder dafs die Gleichungen (33. und 34.) *zugleich* Statt finden, ist nicht möglich; denn diese beiden Gleichungen geben, von einander abgezogen,

$$37.\quad 2 = \mathfrak{G}p,$$

und 2 geht nicht mit p auf.

I. Es kann also nur das *Zweite* Statt finden, nemlich *entweder* die Gleichung (35.), *oder* die Gleichung (36.); und die eine oder die andere *mufs nothwendig* Statt finden, da die aus (30.) folgende Gleichung (32.), aus welcher (35. und 36.) genommen sind, für *jedes* z_φ *nothwendig* Statt hat.

Also ist für *jedes* z_φ, das heifst für *jede* zu $z=p^e$ theilerfremde positive Zahl z_φ, sie mag *kleiner* oder *gröfser* als $z=p^e$ sein (denn für *alle* solche Zahlen gilt der allgemeine *Fermat*sche Satz (§. 87.)), *entweder* $z_\varphi^{\frac{1}{2}\varphi z}=\mathfrak{G}z+1$, *oder* $z_\varphi^{\frac{1}{2}\varphi z}=\mathfrak{G}z-1$, und folglich ist allgemein für jede beliebige zu z theilerfremde Zahl $z_\varphi <$ oder $> z$,

$$38.\quad z_\varphi^{\frac{1}{2}\varphi z}=\mathfrak{G}z\pm1 \quad \text{für} \quad z=p^e;$$

wie es der Lehrsatz in (6.) behauptet.

Dafs nicht die beiden Gleichungen (35. und 36.) für ein- und dasselbe z_φ *zugleich* Statt finden können, ist offenbar, denn die Gleichungen geben, von einander abgezogen,

$$39.\quad 2 = \mathfrak{G}z = \mathfrak{G}e^p,$$

und 2 geht nicht mit e^p auf.

K. Nun erhebe man die Gleichung (2.), in welcher r einer der *Quadratreste* zu $z=p^e$ ist, zur Potenz $\frac{1}{2}\varphi z$, so ergiebt sich

$$40.\quad (x^2)^{\frac{1}{2}\varphi z} = x^{\varphi z} = \mathfrak{G}z+r^{\frac{1}{2}\varphi z}.$$

Aber nach dem allgemeinen *Fermat*schen Lehrsatze ist für *jedes* zu z theilerfremde $x = z_\varphi$,

$$41. \quad x^{\varphi z} = \mathfrak{G}z + 1,$$

also folgt aus (40.)

$$\mathfrak{G}z + 1 = \mathfrak{G}z + r^{\frac{1}{2}\varphi z} \text{ oder}$$

$$42. \quad r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1,$$

das heifst: für *jeden Quadratrest* r ist nothwendig $r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$; wie es der Lehrsatz in (4.) behauptet.

L. Es fragt sich nun, ob auch *Nichtquadratreste* w, $w^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$ geben können. Dieses würde der Fall sein, wenn die Gleichung (42.) für *mehr* als $\frac{1}{2}\varphi z$ Werthe von r aus den Zahlen $z_\varphi > 0$ und $< z$ Statt fände, da es nach (*F.*) nicht mehr als $\frac{1}{2}\varphi z$ Quadratreste r zu $z = p^e$ giebt.

M. Es sei p^k eine beliebige, etwa niedrigere Potenz von p als $z = p^e$ und

$$43. \quad p^k = y.$$

Die zu diesem $y = p^k$ theilerfremden φy Zahlen $y_\varphi > 0$ und $< y$ sind alle diejenigen aus der Reihe 1, 2, 3, 4, ... y, die mit p *nicht aufgehen*. Ihre Anzahl ist nach (§. 81. 7.)

$$44. \quad \varphi y = p^{k-1}(p-1).$$

N. Es sei ferner

$$45. \quad t = p^{k+m} = p^m y$$

eine um m *höhere* Potenz von p als y. Die zu diesem $t = p^{k+m}$ theilerfremden φt Zahlen $t_\varphi > 0$ und $< t$ sind wiederum alle diejenigen aus der Reihe 1, 2, 3, 4, ... t $(= p^m y)$, die mit p *nicht aufgehen*. Ihre Anzahl ist nach (§. 81. 7.)

$$46. \quad \varphi t = p^{k+m-1}(p-1),$$

also p^m *mal so grofs* als die Zahl φy (44.) der zu $y = p^k$ theilerfremden Zahlen > 0 und $< y$, so dafs

$$47. \quad \varphi t = p^m \varphi y$$

ist. Dabei werden *alle* die Zahlen $t_\varphi > 0$ und $< t$ durch

$$48. \quad t_\varphi = ny + y_\varphi$$

ausgedrückt, wo

$$49. \quad n = 0, 1, 2, 3, \dots\, p^m - 1$$

ist, und es giebt keine andern t_φ. Denn allgemein drückt $ny + r$, wo $r > 0$ und $< y$ ist, mit den Werthen (49.) von n *alle* die Zahlen 1, 2, 3, 4, ... t ohne Ausnahme aus, und da nun die t_φ in (49.) diejenigen derselben sein sollen, welche mit p nicht aufgehen, so kann r in $ny + r$ nur diejenigen Zahlen > 0 und $< y$ bezeichnen, welche mit p *nicht aufgehen*, also nur die y_φ; denn

ginge in $ny+r$, r mit p auf, so würden auch die durch $ny+r$ ausgedrückten Zahlen selbst, weil $y=p^k$ mit p aufgeht, durch p theilbar sein; was t_φ nicht sein soll. Ferner giebt es auch eben deshalb *keine andern* t_φ weiter, als die, welche (48. und 49.) ausdrücken. Denn gäbe es andere, so könnten sie durch $ny+r$ nur dann ausgedrückt werden, wenn darin r *nicht mehr* wie y_φ zu $y=p^k$ theilerfremd wäre, sondern mit p aufginge. Diese mit einem *solchen* r ausgedrückten $ny+r$ aber würden mit p aufgehen und folglich keine t_φ sein.

O. Aus (48. und 49.) folgt, dafs nicht blofs nach (47.) überhaupt p^m mal so viele t_φ als y_φ verschieden sind, sondern dafs auch zu *jedem einzelnen* y_φ, p^m zu $t=p^{k+m}$ theilerfremde Zahlen >0 und $<t$ gehören; denn (48.) giebt, weil n vermöge (49.) p^m verschiedene Werthe hat, für *ein- und dasselbe* y_φ, p^m verschiedene t_φ.

P. Nun sei $\varkappa$ irgend eines derjenigen y_φ, für welches

$$50.\quad \varkappa^{\frac{1}{2}\varphi y} = y_\varphi^{\frac{1}{2}\varphi y} = \mathfrak{G}y+1$$

ist, und λ nirgend eines derjenigen y_φ, für welches

$$51.\quad \lambda^{\frac{1}{2}\varphi y} = y_\varphi^{\frac{1}{2}\varphi y} = \mathfrak{G}y-1$$

ist. Eines oder das Andere ist für *jedes* y_φ der Fall, so dafs $\varkappa$ und λ *alle* $y_\varphi>0$ und $<y$ bezeichnen. Denn da nach (6.) $z_\varphi^{\frac{1}{2}\varphi z}=\mathfrak{G}z\pm1$ für *alle* z_φ ist, und für $z=p^e$ (1.), so ist auch für *alle* y_φ,

$$52.\quad y_\varphi^{\frac{1}{2}\varphi y} = \mathfrak{G}y\pm1$$

für $y=p^k$ (43.).

Zu *jedem* $\varkappa=y_\varphi$ gehören nun nach (*O.*) p^m und zu *jedem* $\lambda=y_\varphi$ p^m verschiedene t_φ, die durch (48. und 49.) ausgedrückt werden. Bezeichnet man also erstere durch τ, letztere durch σ, so ist nach (48.)

$$53.\quad \tau = ny+\varkappa \text{ und}$$

$$54.\quad \sigma = ny+\lambda,$$

und τ und σ bezeichnen nun zusammen *alle* vorhandenen t_φ.

Aber eben wie nach (6.) für $z=p^e$ (1.), $z_\varphi^{\frac{1}{2}\varphi z}=\mathfrak{G}z\pm1$ ist, ist auch für $t=p^{k+m}$,

$$55.\quad t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{G}t\pm1,$$

oder, da $\varphi t=p^m\varphi y$ ist (47.),

$$56.\quad t_\varphi^{\frac{1}{2}p^m\varphi y} = \mathfrak{G}t\pm1$$

und, wenn man hierin den Ausdruck (48.) von t_φ setzt,

$$57.\quad t_\varphi^{\frac{1}{2}\varphi t} = t_\varphi^{\frac{1}{2}p^m\varphi y} = (ny+y_\varphi)^{\frac{1}{2}p^m\varphi y} = \mathfrak{G}y+y_\varphi^{\frac{1}{2}p^m\varphi y}.$$

Giebt man in dieser Gleichung dem y_φ rechterhand die Werthe $\varkappa$ (50.), zu deren jedem p^m verschiedene Werthe von $\tau = t_\varphi$ gehören, so erhält man aus (50.)

$$58.\quad t_\varphi^{\frac{1}{2}\varphi t} = \tau^{\frac{1}{2}\varphi t} = \mathfrak{S}y + (\mathfrak{S}y+1)^{p^m} = \mathfrak{S}y + 1$$

für *alle* $\tau = t_\varphi$; und giebt man in (57.) dem y_φ rechts die Werthe λ (51.), zu deren jedem p^m verschiedene Werthe von $\sigma = t_\varphi$ gehören, so giebt (51.)

$$59.\quad t_\varphi^{\frac{1}{2}\varphi t} = \sigma^{\frac{1}{2}\varphi t} = \mathfrak{S}y + (\mathfrak{S}y-1)^{p^m} = \mathfrak{S}y - 1,$$

letzteres weil p und folglich p^m *ungerade* ist.

Es folgt also, dafs alle die p^m zu jedem $y_\varphi = \varkappa$ gehörigen Werthe τ von t_φ, zur Potenz $\frac{1}{2}\varphi t$ erhoben, $\mathfrak{S}y+1$, und alle die p^m zu jedem $y_\varphi = \lambda$ gehörigen Werthe σ von t_φ, zur Potenz $\frac{1}{2}\varphi t$ erhoben, $\mathfrak{S}y-1$ geben.

Q. Jene zu den $y_\varphi = \varkappa$ gehörigen Werthe τ von t_φ können aber *nur diejenigen* t_φ in (55.) sein, welche *zugleich*

$$60.\quad t_\varphi^{\frac{1}{2}\varphi t} = \tau^{\frac{1}{2}\varphi t} = \mathfrak{S}t + 1$$

geben, und die zu den $y_\varphi = \lambda$ gehörigen Werthe σ von t_φ *nur diejenigen* t_φ in (55.), für welche *zugleich*

$$61.\quad t_\varphi^{\frac{1}{2}\varphi t} = \sigma^{\frac{1}{2}\varphi t} = \mathfrak{S}t - 1$$

ist: denn wäre es anders und z. B. nach (58. und 61.) *zugleich* für ein- und dasselbe t_φ

$$62.\quad \begin{cases} t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}y + 1 \text{ und} \\ t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}t - 1, \end{cases}$$

so müfste, Eins vom Andern abgezogen,

$$63.\quad 0 = \mathfrak{S}y - \mathfrak{S}t + 2$$

sein, also müfste, da y und t beide mit p aufgehen, auch 2 mit p aufgehen; was nicht der Fall ist. Aus gleichem Grunde kann nicht nach (59 und 60.) *zugleich* für ein- und dasselbe t_φ,

$$64.\quad \begin{cases} t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}y - 1 \text{ und} \\ t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}t + 1 \end{cases}$$

sein. Es kann also nur für ein- und dasselbe t_φ *zugleich,*

$$65.\quad t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}y + 1 \text{ und } t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}t + 1 \text{ oder}$$

$$66.\quad t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}y - 1 \text{ und } t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{S}t - 1$$

sein. Und da nun die Werthe τ von t_φ nach (58.) $\tau^{\frac{1}{2}\varphi t} = \mathfrak{S}y + 1$ und die Werthe σ von t_φ nach (59.) $\sigma^{\frac{1}{2}\varphi t} = \mathfrak{S}y - 1$ geben, so kann nur Statt finden, was die Gleichungen (60. und 61.) ausdrücken.

Es folgt demnach, dafs nur diejenigen Werthe τ von t_φ, welche nach (48.) zu den $y_\varphi = \varkappa$ (50.) gehören, $t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{G}t+1$, und *nur* diejenigen Werthe σ von t_φ, welche nach (48.) zu den $y_\varphi = \lambda$ (51.) gehören, $t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{G}t-1$ geben können; wobei zugleich die τ und die σ zusammen die *sämmtlichen* Werthe von t_φ sind. Und da nun zu jedem $y_\varphi = \varkappa$ und zu jedem $y_\varphi = \lambda$ p^m verschiedene Werthe von t_φ gehören, so folgt, dafs es p^m *mal so viele* Werthe τ von t_φ giebt, die die Gleichung (60.) erfüllen, als $y_\varphi = \varkappa$ vorhanden sind, die der Gleichung (37.) genugthun, und p^m *mal so viele* Werthe σ von t_φ, die der Gleichung (61.) genugthun, als es $y_\varphi = \lambda$ giebt, die die Gleichung (51.) erfüllen.

Man wird demnach die Anzahl der Werthe τ und σ von t_φ finden, wenn man die Zahl der Werthe $\varkappa$ und λ von y_φ für $y = p^k$ *für irgend einen Werth von k* kennt; man darf den letzten nur mit p^m multipliciren.

R. Für $k = 1$ in $y = p^k$ (43.), nemlich für

$$67. \quad y = p,$$

ist aber die Zahl der $y_\varphi = \varkappa$ und der $y_\varphi = \lambda$, welche $\varkappa^{\frac{1}{2}\varphi y} = \mathfrak{G}y+1$ und $\lambda^{\frac{1}{2}\varphi y} = \mathfrak{G}y-1$ geben, wirklich bekannt. Hier ist nemlich $\frac{1}{2}\varphi y = \frac{1}{2}\varphi p = \frac{1}{2}(p-1)$; alle ***Quadratreste*** r zu p geben nach (§. 49.) $r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, und alle ***Nichtquadratreste*** ϱ zu p geben $\varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$. Also sind die Quadratreste r die hiesigen $\varkappa$ und die Nichtquadratreste ϱ die hiesigen λ. Sodann ist nach (§. 45.) die Zahl der Quadratreste der Zahl der Nichtquadratreste *gleich*, also die Zahl von beiden $\frac{1}{2}(p-1)$. Folglich giebt es für $\varkappa = 1$ $\frac{1}{2}(p-1)$ Werthe $\varkappa$ von y_φ, die die Gleichung (50.), und $\frac{1}{2}(p-1)$ Werthe λ von y_φ, die die Gleichung (51.) erfüllen.

Demnach giebt es denn also für

$$68. \quad t = p^{m+1} \text{ (32.)},$$

da jetzt in (45.) $k = 1$ gesetzt worden ist, vermöge (*Q.*),

69. $\frac{1}{2}(p-1).p^m$ Werthe τ von t_φ, für welche $t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{G}t+1$ ist (60.) und

70. $\frac{1}{2}(p-1).p^m$ Werthe σ von t_φ, für welche $t_\varphi^{\frac{1}{2}\varphi t} = \mathfrak{G}t-1$ ist (61.).

S. Man setze nun in (68.) $m+1 = e$ oder $m = e-1$, so geht t (68.) in z (1.) über und es folgt also aus (69. und 70.), dafs es

71. $\frac{1}{2}(p-1).p^{e-1}$ Werthe von z_φ giebt, für welche $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z+1$, und

72. $\frac{1}{2}(p-1).p^{e-1}$ Werthe von z_φ, für welche $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z-1$ ist.

Aber nach (§. 7.) ist

$$73. \quad \tfrac{1}{2}(p-1)p^{e-1} = \tfrac{1}{2}\varphi p^e = \tfrac{1}{2}\varphi z:$$

also giebt es nach (71. und 72.)

74. $\frac{1}{2}\varphi z$ Werthe von z_φ, für welche $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$, und

75. $\frac{1}{2}\varphi z$ Werthe von z_φ, für welche $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ ist.

T. Nun war nach (*K.*) für *sämmtliche Quadratreste* $r = z_\varphi$, $r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$, und die *Anzahl* der Quadratreste ist nach (*E.*) $= \frac{1}{2}\varphi z$: also folgt schliefslich, weil von den überhaupt vorhandenen φz Werthen von z_φ nur noch die $\frac{1}{2}\varphi z$ *Nichtquadratreste* übrig bleiben, dafs für *diese*, gemäfs (75.), $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ ist. Dieses ist was der Lehrsatz in (5.) behauptet.

U. *a.* Übrigens, wenn eine zu z theilerfremde Zahl z_φ, die *gröfser* als z ist, ein *Quadratrest* zu z sein soll, so kann sie nur durch

76. $$z_\varphi = \mathfrak{G}z + r$$

ausgedrückt werden, wo r eine der Zahlen $z_\varphi > 0$ und $< z$ und *Quadratrest* zu z ist. Denn gesetzt x sei die Zahl, welche den vorausgesetzten Quadratrest z_φ giebt, so mufs

77. $$x^2 = \mathfrak{G}z + z_\varphi$$

sein. Wäre nun in (77.) z_φ nicht nach (76.) $= \mathfrak{G}z + r$, so könnte nur

78. $$z_\varphi = \mathfrak{G}z + w$$

sein, wo w eine der Zahlen $z_\varphi > 0$ und $< z$ und *Nichtquadratrest* zu z ist. Dann aber wäre in (77.)

79. $$x^2 = \mathfrak{G}z + \mathfrak{G}z + w = \mathfrak{G}z + w$$

und es gäbe also eine Zahl x, deren *Quadrat* zu z den *Nichtquadratrest* w liefse; was nicht sein kann.

b. Eben so kann eine zu z theilerfremde Zahl z_φ, die *gröfser* als z ist, wenn sie *Nichtquadratrest* zu z sein soll, nur durch

80. $$z_\varphi = \mathfrak{G}z + w$$

ausgedrückt werden, wo w eine der Zahlen $z_\varphi > 0$ und $< z$ und *Nichtquadratrest* zu z ist. Denn gesetzt es wäre nicht wie in (80.) $z_\varphi = \mathfrak{G}z + w$, so könnte nur

81. $$z_\varphi = \mathfrak{G}z + r$$

sein, wo r eine der Zahlen $z_\varphi > 0$ und $< z$ und *Quadratrest* zu z ist. Dann aber gäbe es nach (*a.*) eine Zahl x, für welche

82. $$x^2 = \mathfrak{G}z + z_\varphi$$

ist und z_φ wäre also nicht *Nichtquadratrest* zu z, sondern *Quadratrest*; gegen die Voraussetzung.

c. Also *alle* zu z theilerfremden Zahlen $z_\varphi > z$, welche *Quadratreste* zu z sind, werden nur durch $z_\varphi = \mathfrak{G}z + r$ ausgedrückt, wo r ein

Quadratrest zu z und $< z$ ist, und alle zu z theilerfremden Zahlen $z_\varphi > z$, welche *Nichtquadratreste* zu z sind, nur durch $z_\varphi = \mathfrak{S}z + w$, wo w ein *Nichtquadratrest* zu z und $< z$ ist.

Nun ist aber

83. $z_\varphi^{\frac{1}{2}\varphi z} = (\mathfrak{S}z + r)^{\frac{1}{2}\varphi z} = \mathfrak{S}z + r^{\frac{1}{2}\varphi z}$ und

84. $z_\varphi^{\frac{1}{2}\varphi z} = (\mathfrak{S}z + w)^{\frac{1}{2}\varphi z} = \mathfrak{S}z + w^{\frac{1}{2}\varphi z}$.

Setzt man hierin (4. und 5.), so ergiebt sich

85. $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{S}z + \mathfrak{S}z + 1 = \mathfrak{S}z + 1$ für die $z_\varphi > z$, welche *Quadratreste* zu z sind und

86. $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{S}z + \mathfrak{S}z - 1 = \mathfrak{S}z - 1$ für die $z_\varphi > z$, welche *Nichtquadratreste* zu z sind; und folglich gelten die Gleichungen (4. und 5.) auch für die r und w, welche *gröſser* als z sind.

Beweis von II. *V.* Wäre ein *Nichtquadratrest* w zu p nicht auch Nichtquadratrest zu p^e, so könnte er nur *Quadratrest* zu p sein, denn *theilerfremd* auch zu p^e ist jedes zu p theilerfremde w. Es müſste also dann eine Zahl x geben, für welche

88. $x^2 = \mathfrak{S}p^e + w$

wäre. Diese Gleichung heiſst aber eben so viel als

89. $x^2 = \mathfrak{S}p + w$,

denn $\mathfrak{S}p^e$ ist immer ein ganzzahliges Vielfache von p. Also wäre nach (89.) w nicht ein *Nichtquadratrest*, sondern ein Quadratrest zu p; gegen die Voraussetzung. Mithin sind alle *Nichtquadratreste* zu p auch zugleich *Nichtquadratreste* zu p^e, was zunächst (II.) behauptet.

W. Für jeden *Nichtquadratrest* w zu $z = p^e$ ist nach (5.)

90. $w^{\frac{1}{2}\varphi z} = \mathfrak{S}z - 1 = \mathfrak{S}p^e - 1$,

oder, da nach (§. 81. 7.) $\frac{1}{2}\varphi z = \frac{1}{2}p^{e-1}(p-1)$ ist und $\mathfrak{S}p^e$ auch durch $\mathfrak{S}p$ ausgedrückt wird,

91. $w^{\frac{1}{2}p^{e-1}(p-1)} = \mathfrak{S}p - 1$.

Wäre nun w nicht ein *Nichtquadratrest* zu p, so müſste es ein *Quadratrest* zu p sein, denn *theilerfremd* auch zu p ist jedes zu p^e theilerfremde w. Dann aber wäre nach (§. 49. 1.)

92. $w^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1$.

Dieses zur Potenz p^{e-1} erhoben giebt

93. $w^{\frac{1}{2}p^{e-1}(p-1)} = (\mathfrak{S}p + 1)^{p^{e-1}} = \mathfrak{S}p + 1$

statt daſs nach (91.) $w^{\frac{1}{2}p^{e-1}(p-1)} = \mathfrak{S}p - 1$ sein soll. Also kann w nicht *Qua-*

dratrest zu p sein, und folglich ist auch umgekehrt jeder *Nichtquadratrest* w zu p^e auch *Nichtquadratrest* zu p; wie es ferner (II.) behauptet.

X. a. Die beliebige Zahl Z werde wie in (§. 96.) durch

$$94.\quad Z = 2^m . p_1^{e_1} . p_1^{e_2} . p_3^{e_3} \dots . p_\mu^{e_\mu}$$

ausgedrückt. Es sei w einer der *Nichtquadratreste* zu p_1 und $< p_1$. Alsdann sind nach (*U. b.*) auch alle durch

$$95.\quad W = n_1 p_1 + w$$

ausgedrückte Zahlen, wo n_1 eine ganz beliebige ganze Zahl ist, *Nichtquadratreste* zu p_1.

Die in (II.) bezeichnete Gröfse P ist hier

$$96.\quad P = 2p_2 . p_3 . p_4 \dots . p_\mu,$$

denn sie soll das Product der ersten Potenzen aller der Stammfactoren sein, die Z (94.) noch aufser p_1 enthält. Diese Gröfse P ist zu p_1 *theilerfremd*, denn sie enthält den Stammfactor p_1 nicht.

b. Nun setze man *willkürlich* die Gleichung

$$97.\quad W = n_1 p_1 + w \text{ (95.)} = n_2 P + 1,$$

welche

$$98.\quad n_2 P = n_1 p_1 + w - 1$$

giebt. Für diese *willkürliche* Gleichung findet nach (§. 34.), weil P und p_1 *theilerfremd* sind (*a.*), für n_2 immer ein ganzzahliger positiver Werth >0 und $<p_1$ und für n_1 ein ganzzahliger positiver Werth >0 und $<P$ Statt. Also ist $n_1 p_1$ immer $< Pp_1$ und höchstens $=(P-1)p_1$, und folglich ist in (95.) W höchstens $=(P-1)p_1 + w$, mithin, da $w < p_1$ sein soll, $W < Pp_1$ und folglich jedenfalls

$$99.\quad W < z;$$

denn Z (94.) ist vermöge (96.) $= Pp_1 . 2^{m-1} . p_1^{e_1-1} . p_2^{e_2-1} \dots . p_\mu^{e_\mu-1}$.

c. Nun soll vermöge (97.) *zugleich*

$$100.\quad W = n_1 p_1 + w \text{ und}$$

$$101.\quad W = n_2 P + 1 \text{ sein.}$$

Aus (100.) folgt, dafs W nicht mit p_1 aufgeht; denn $w < p_1$ geht damit nicht auf, und aus (101.) folgt, dafs W mit keinem der Stammfactoren >1 von P aufgeht, die alle die übrigen Stammfactoren sind, welche Z noch aufser p_1 enthält, denn 1 geht mit keinem dieser Factoren auf. Also folgt aus (100. und 101.), dafs W mit keinem einzigen der Stammfactoren >1 von Z aufgeht und folglich zu Z *theilerfremd* ist

d. Nun kann W kein *Quadratrest* zu Z sein. Denn wäre dies der Fall, so müfste es eine zu Z und folglich auch zu p_1 theilerfremde Zahl x geben, für welche

$$102. \quad x^2 = \mathfrak{S}Z + W$$

wäre. Diese Gleichung zur Potenz $\frac{1}{2}(p-1)$ erhoben, giebt

$$103. \quad x^{p-1} = (\mathfrak{S}Z + W)^{\frac{1}{2}(p_1-1)} = \mathfrak{S}Z + W^{\frac{1}{2}(p-1)},$$

oder, da $\mathfrak{S}Z$ vermöge (94.) auch durch $\mathfrak{S}p_1$ ausgedrückt werden kann,

$$104. \quad x^{p-1} = \mathfrak{S}p_1 + W^{\frac{1}{2}(p_1-1)}.$$

Aber W ist *Nichtquadratrest* zu p_1 (*a.*), und für alle *Nichtquadratreste* zu der Stammzahl p_1 ist nach (§. 49. 1.)

$$105. \quad W^{\frac{1}{2}(p_1-1)} = \mathfrak{S}p_1 - 1:$$

also wäre in (104.)

$$106. \quad x^{p_1-1} = \mathfrak{S}p_1 + \mathfrak{S}p_1 - 1 = \mathfrak{S}p_1 - 1.$$

Nach dem allgemeinen *Fermat*schen Satze (§. 40.) ist aber für *alle möglichen* zu p_1 theilerfremden Zahlen:

$$107. \quad x^{p_1-1} = \mathfrak{S}p_1 + 1;$$

also kann W nicht *Quadratrest* zu Z sein und ist folglich nothwendig *Nichtquadratrest* zu Z.

e. Es giebt daher, wenn p_1 einer der Stammfactoren zu der beliebigen Zahl Z ist, immer Zahlen $W > 0$ und $< Z$ (99.), die durch (100. und 101.) oder durch (7. und 8.) ausgedrückt werden, wo w einer der *Nichtquadratreste* zu p_1 und > 0 und $< p_1$ ist, die zu p_1 und Z *zugleich Nichtquadratreste* sind; wie es (II.) behauptet.

Y. Anmerkung. Zu erinnern ist, dafs die Behauptungen (I.) des Lehrsatzes nur für den Fall nothwendig gelten, wo z, wie in (1.) vorausgesetzt, irgend eine Potenz mit positivem ganzzahligen Exponenten von einer *ungeraden Stammzahl* p ist, oder, was dasselbe ist, nur den einen Stammtheiler $p > 2$ hat. Denn hätte z mehrere solche Stammtheiler, oder auch nur den einen Stammtheiler 2, so würden diejenigen Schlüsse in (*D.*) und weiter, bei welchen vorausgesetzt wird, dafs p eine Stammzahl > 2 sei und z nur diesen einen Stammtheiler haben solle, *nicht* Statt finden.

§. 98.

Lehrsatz.

Wenn in der Gleichung

$$1. \quad z = 2^m$$

m *eine beliebige positive ganze Zahl* > 1 *ist und man bezeichnet die zu*

z *theilerfremden Zahlen* >0 *und* $<$ z, *welche hier die sämmtlichen* ***ungeraden Zahlen***

$$2. \quad 1, 3, 5, 7, 9, \ldots\ldots z-1$$

sind, wie immer durch z_φ, *ihre* ***Anzahl*** *durch* φz, *so ist für* ***jedes*** $m>1$ *und für* ***jedes*** z_φ, *sei es* ***Quadratrest*** *oder* ***Nichtquadratrest*** *zu* z,

$$3. \quad z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z+1;$$

mit der ***einzigen Ausnahme*** *der Zahl*

$$4. \quad z_\varphi = 3 \text{ für } m=2, \text{ also für } z=2^2=4,$$

für welche

$$5. \quad z_\varphi^{\frac{1}{2}\varphi z} = 3^1 = \mathfrak{G}z-1 \text{ ist.}$$

Nichtquadratreste *zu* $z=2^m$ *giebt es übrigens immer, für jedes* $m>1$.

Beispiel. Es sei

$$6. \quad m=4, \text{ also } z=2^4=16.$$

Dann sind die zu z theilerfremden Zahlen >0 und $<z$ folgende:

$$7. \quad z_\varphi = 1, 3, 5, 7, 9, 11, 13 \text{ und } 15,$$

und ihre Anzahl ist

$$8. \quad \varphi z = 8, \text{ also ist } \tfrac{1}{2}\varphi z = 4.$$

Nun findet sich $1^4 = \mathfrak{G}.16+1$, $3^4 = 81 = \mathfrak{G}.16+1$, $5^4 = 25^2 = (\mathfrak{G}.16+9)^2 = \mathfrak{G}.16+81 = \mathfrak{G}.16+1$, $7^4 = 49^2 = (\mathfrak{G}.16+1)^2 = \mathfrak{G}.16+1$, $9^4 = 81^2 = (\mathfrak{G}.16+1)^2 = \mathfrak{G}.16+1$, $11^4 = 121^2 = (\mathfrak{G}.16+9)^2 = \mathfrak{G}.16+81 = \mathfrak{G}.16+1$, $13^4 = 169^2 = (\mathfrak{G}.16+9)^2 = \mathfrak{G}.16+81 = \mathfrak{G}.16+1$, $15^4 = (\mathfrak{G}.16-1)^4 = \mathfrak{G}.16+1$; der Gleichung (3.) gemäfs.

Dafs nach (5.) $3^1 = \mathfrak{G}.4-1$ sei, ist offenbar.

Die Zahlen (7.) quadrirt geben der Reihe nach $1^2, 3^2, 5^2, 7^2, 9^2, 11^2, 13^2, 15^2 = \mathfrak{G}.16+1, 9, 9, 1, 1, 9, 9$ und 1, also sind hier von den Zahlen z_φ (7.) nur die beiden 1 und 9 *Quadratreste*, die übrigen 3, 5, 7, 11, 13 und 15 sind *Nichtquadratreste*.

Beweis. *A.* Dafs zuerst die z_φ hier alle die *ungeraden* Zahlen (2.) sind, ist leicht zu sehen; denn $z=2^m$ hat nur den einen Stammtheiler 2, und diesen hat keine der ungeraden Zahlen (2.); also sind sie zunächst sämmtlich zu $z=2^m$ theilerfremd. Es giebt aber auch *keine andern* z_φ. Denn andere z_φ könnten nur *gerade* Zahlen sein, und alle diese gehen mit dem Stammtheiler 2 von $z=2^m$ auf und sind folglich zu $z=2^m$ *nicht* theilerfremd.

B. Für $m=2$, also $z=2^2=4$, giebt es nur die beiden zu z theilerfremden Zahlen 1 und 3 >0 und $<z$. Die Anzahl φz der z_φ ist also

hier $=2$, folglich ist $\frac{1}{2}\varphi z = 1$, und $1^{\frac{1}{2}\varphi z} = 1^1 = 1$ erfüllt noch die Gleichung (3.); hingegen 3 giebt $3^{\frac{1}{2}\varphi z} = 3^1 = 3 = \mathfrak{G}z - 1$; gemäfs (5.).

C. Da hier z_φ nie etwas anderes als eine *ungerade* Zahl sein kann, so kann *jedes* z_φ für *jedes* m durch

$$9. \quad z_\varphi = 4n \pm 1 = 2^2.n \pm 1$$

ausgedrückt werden (§. 10.).

Quadrirt man die Gleichung (9.) wiederholt, so ergiebt sich, sie selbst hinzugeschrieben:

$$10. \begin{cases} z_\varphi = 2^2.n \pm 1, \\ z^{2^1} = (2^2.n \pm 1)^2 = 2^4.n \pm 2^3.n + 1 = \mathfrak{G}.2^3 + 1, \\ z^{2^2} = (\mathfrak{G}.2^3 + 1) = \mathfrak{G}^2.2^6 + 2\mathfrak{G}.2^3 + 1 = \mathfrak{G}.2^4 + 1, \\ z^{2^3} = (\mathfrak{G}.2^4 + 1) = \mathfrak{G}^2.2^8 + 2\mathfrak{G}.2^4 + 1 = \mathfrak{G}.2^5 + 1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Bei jeder neuen Quadrirung kommt $\mathfrak{G}$mal die zugehörige Potenz von 2, 2 *mal genommen* vor, und dieses Glied bestimmt die Potenz von 2 zu dem neuen $\mathfrak{G}$, die also um 1 höher ist als die vorigen. Andrerseits steigt bei jeder Quadrirung auch der Exponent der 2 in dem Exponenten von z_φ linkerhand ebenfalls um 1: also steigen die Exponenten der 2 rechts und die Exponenten der 2 in dem Exponenten von z_φ links stets um *gleich viel,* mithin beide gleichmäfsig, z. B. durch k Quadrirungen um k. Nun ist in der *zweiten* Gleichung (10.) der Exponent 3 von 2 rechts um 2 gröfser als der Exponent 1 der 2 in dem Exponenten von z_φ. Erreicht also der Exponent der 2 rechts die Zahl m, so wird der Exponent der 2 in dem Exponenten der 2 von z_φ links die Zahl $m-2$ erreicht haben, und folglich ist allgemein für jedes m

$$11. \quad z_\varphi^{2^{m-2}} = \mathfrak{G}.2^m + 1.$$

Aber 2^m ist z selbst (1.), also giebt (11.)

$$12. \quad z_\varphi^{2^{m-2}} = \mathfrak{G}z + 1.$$

D. Nach (§. 81. 7.) ist aber

$$13. \quad \varphi z = \varphi.2^m = 2^{m-1}.1 = 2^{m-1},$$

also ist

$$14. \quad \tfrac{1}{2}\varphi z = \tfrac{1}{2}.2^{m-1} = 2^{m-2}.$$

Es ist demnach, (14.) in (12.) gesetzt,

$$15. \quad z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1,$$

für jedes z_φ und jedes $m > 1$; gemäfs (3.).

E. Ausgenommen ist indessen der Fall $m = 2$. Für diesen gilt nur die *erste* Gleichung (10.), und diese wird auch für $z_\varphi = 1$ und 3 gehörig erfüllt; wie es sich in (*B.*) zeigte.

F. Dafs es zu $z = 2^m$ *immer Nichtquadratreste* und *mindestens* $\frac{1}{2}\varphi z$ *Nichtquadratreste* unter den φz Zahlen $z_\varphi > 0$ und $< z$ gebe, ist (§. 90. VI.) gemäfs.

§. 99.

Lehrsatz.

Man bezeichne wie in (§. 92.) *das* ***Product*** *der sämmtlichen zu einer beliebigen Zahl* z ***theilerfremden*** *Zahlen* >0 *und* $<$ z *durch* Z, *durch* p *eine beliebige* ***Stammzahl*** >2 *und durch* e *eine beliebige ganze positive Zahl. Alsdann ist*

1. $Z = \mathfrak{G}z - 1$ *für* $z = 4$, $z = p^e$, $z = 2p^e$, und
2. $Z = \mathfrak{G}z + 1$ *für jedes andere* z.

Dieses ist der ***verallgemeinerte Wilsonsche Satz*** (§. 48.). *Denn für den besondern Fall* $e = 1$ *in* $z = p^e$ (1.) *ist er es selbst.*

Beispiele. 1. Für $z = 4$ sind die zu z *theilerfremden* Zahlen 1 und 3, und $Z = 1.3 = 3$ ist $= \mathfrak{G}z - 1$; gemäfs (1.).

2. Für $p = 3$, $e = 2$, also $z = p^e = 9$, sind die zu z theilerfremden Zahlen 1, 2, 4, 5, 7, 8, und es ist $Z = 1.2.4.5.7.8 = 2240 = 249.9 - 1 = \mathfrak{G}z - 1$; gemäfs (1.).

3. Für $p = 3$, $e = 2$, also $z = 2p^e = 18$, sind die zu z theilerfremden Zahlen 1, 5, 7, 11, 13, 17, und ihr Product Z ist $= 85085 = 4727.18 - 1 = \mathfrak{G}z - 1$; gemäfs (1.).

4. Zu $z = 15$ sind die Zahlen 1, 2, 4, 7, 8, 11, 13, 14 theilerfremd, und ihr Product Z ist $= 896896 = 59793.15 + 1 = \mathfrak{G}z + 1$; gemäfs (2.).

Erster Beweis. *A.* Nach (§. 92. 4. und 5.) ist $Z = \mathfrak{G}z - 1$, wenn die Anzahl n der Werthenpaare von x, die der Gleichung

$$3. \quad x^2 = \mathfrak{G}z + 1$$

genugthun, *ungerade*, und $Z = \mathfrak{G}z + 1$, wenn n *gerade* ist.

B. Es sei nun zuerst $z = 4$ (1.), so ist, dieses z mit dem (§. 94. 1.) verglichen,

$$4. \quad m = 2, \quad \mu = 0,$$

also für diesen Fall gemäfs (§. 96. 5.) $n = 2^0 = 1$, mithin n *ungerade*, und folglich $Z = \mathfrak{G}z - 1$; gemäfs (1.).

C. Es sei zweitens $z = p^e$ (1.), so ist, dieses z mit dem (§. 96. 1.) verglichen,

$$5. \quad m = 0, \quad \mu = 1,$$

also für diesen Fall gemäfs (§. 96. 3.) $n = 2^0 = 1$, mithin n wiederum *ungerade* und folglich $Z = \mathfrak{G}z - 1$; gemäfs (1.).

D. Es sei drittens $z = 2p^e$ (1.), so ist, dieses z mit dem (§. 96. 1.) verglichen,

$$6. \quad m = 1, \quad \mu = 1,$$

also für diesen Fall gemäfs (§. 96. 4.) $n = 2^0 = 1$, mithin n abermals *ungerade* und folglich $Z = \mathfrak{G}z - 1$; gemäfs (1.).

E. Alle andern z als $z = 4$, p^e und $2p^e$ (1.) sind in folgenden Fällen begriffen:

7.
- *a.* $m = 0$, $\mu = 2, 3, 4, \ldots$, und für diese Fälle ist nach (§. 96. 3.)
 $$7. \quad n = 2^{1,2,3,\ldots}, \text{ also } n \text{ immer } gerade;$$
- *b.* $m = 1$, $\mu = 2, 3, 4, \ldots$, und für diese Fälle ist nach (§. 96. 4.)
 $$8. \quad n = 2^{1,2,3,\ldots}, \text{ also } n \text{ immer } gerade;$$
- *c.* $m = 2$, $\mu = 1, 2, 3, \ldots$, und für diese Fälle ist nach (§. 96. 5.)
 $$9. \quad n = 2^{1,2,3,\ldots}, \text{ also } n \text{ immer } gerade;$$
- *d.* $m > 2$, $\mu = 0, 1, 2, 3, \ldots$, und für diese Fälle ist nach (§. 96. 6.)
 $$10. \quad n = 2^{1,2,3,\ldots}, \text{ also } n \text{ immer } gerade.$$

Also ist für *alle* andern z als $z = 4$, p^e und $2p^e$, $Z = \mathfrak{G}z + 1$; gemäfs (2.).

Zweiter Beweis. *F.* Man setze wie in (§. 95.) den *allgemeinen* Ausdruck von z,

$$8. \quad z = 2^m . p_1^{e_1} . p_2^{e_2} . p_3^{e_3} \ldots . p_\mu^{e_\mu}.$$

Für jeden *Nichtquadratrest* w zu z ist nach (§. 92. 7.)

$$9. \quad Z = \mathfrak{G}z + w^{\frac{1}{2}\varphi z}.$$

Es kommt also nur darauf an, was $w^{\frac{1}{2}\varphi z}$ für die verschiedenen Zusammensetzungsarten von z ist.

G. Erstlich. Es sei in (8.)

$$10. \quad m = 1, \quad \mu = 0, \text{ also blofs } z = 2.$$

Hier giebt es nur die einzige zu z theilerfremde Zahl $z_\varphi = 1$; also ist auch $Z = 1$ und folglich

$$11. \quad Z = \mathfrak{G}z + 1 \text{ für } z = 2.$$

H. Zweitens. Es sei in (8.)

$$12. \quad m = 2, \quad \mu = 0, \quad \text{also} \quad z = 2^2 = 4.$$

Hier giebt es nur die zwei zu z theilerfremden Zahlen $z_\varphi = 1$ und $3 > 0$ und $< z$; also ist $Z = 1.3 = 3 = 4 - 1$ und folglich

$$13. \quad Z = \mathfrak{G}z - 1 \text{ für } z = 2^2 = 4.$$

I. ***Drittens.*** Es sei in (8.)

$$14.\quad m > 2,\quad \mu = 0,\quad \text{also}\quad z = 2^m.$$

Nimmt man aus den zu z theilerfremden Zahlen $z_\varphi > 0$ und $< z$ irgend einen *Nichtquadratrest* w, deren es nach (§. 98.) immer giebt, so ist nach (§. 98. 3.)

$$15.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1,$$

also ist für $z = 2^m$ und $m > 2$ gemäfs (9.)

$$16.\quad Z = \mathfrak{G}z + \mathfrak{G}z + 1 \text{ für jedes } m > 2 \text{ in } z = 2^m.$$

K. ***Viertens.*** Es sei in (8.)

$$17.\quad m = 0,\quad \mu = 1,\quad \text{also}\quad z = p^e.$$

Nimmt man hier wieder aus den zu z theilerfremden Zahlen $z_\varphi > 0$ und $< z$ irgend ein *Nichtquadratrest*, deren es nach (§. 97.) immer $\frac{1}{2}\varphi z$ giebt, so ist nach (§. 97. 5.)

$$18.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1:$$

also ist für $z = p^e$ gemäfs (9.)

$$19.\quad Z = \mathfrak{G}z + \mathfrak{G}z - 1 = \mathfrak{G}z - 1 \text{ für jede Stammzahl } p > 2 \text{ und jedes } e > 0 \text{ in } p^e.$$

L. ***Fünftens.*** Es sei in (8.)

$$20.\quad m = 1,\quad \mu = 1,\quad \text{also}\quad z = 2p^e.$$

Es giebt nach (§. 97. II.) immer zu $2p^e$ theilerfremde Zahlen w, die zu $2p^e$ und p^e *zugleich Nichtquadratreste* sind. Sie werden durch die beiden Gleichungen (7. und 8. §. 97.) ausgedrückt, und da das dortige P in (§. 97. 8.), als das Product der Stammtheiler, welche z noch aufser p hat, hier $= 2$ ist, so sind die w in (§. 97. 8.) immer *ungerade;* wie es auch nothwendig ist, da *alle* zu $2p^e$ *theilerfremden Zahlen,* also auch die Nichtquadratreste, den Theiler 2 von $2p^e$ nicht haben können und folglich nothwendig *alle* ungerade sein müssen. Unter den *ungeraden* Nichtquadratresten w zu $2p^e$ giebt es also gemäfs (§. 97. II.) solche, die *zugleich* Nichtquadratreste zu p^e sind. Für diese ist dann nach (97. 5.)

$$21.\quad w^{\frac{1}{2}\varphi p^e} = \mathfrak{G}p^e - 1.$$

Nun ist aber nach (§. 81. 7.)

$$22.\quad \tfrac{1}{2}\varphi p^e = \tfrac{1}{2}p^{e-1}(p-1) \text{ und auch } \tfrac{1}{2}\varphi(2p^e) = \tfrac{1}{2}p^{e-1}(p-1);$$

also ist auch für das gegenwärtige $z = 2p^e$, $\frac{1}{2}\varphi z = \frac{1}{2}p^{e-1}p - 1 = \frac{1}{2}\varphi p^e$, mithin in (21.)

$$23.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}p^e - 1.$$

Es ist aber w eine *ungerade* Zahl, also ist vermöge (23.), was auch $\frac{1}{2}\varphi z$ sein mag, $\mathfrak{G}p^e$ nothwendig *gerade*, und folglich, da p^e immer *ungerade* ist, was auch e sein mag, $\mathfrak{G}$ nothwendig *gerade.* Es mufs also in (23.) $\mathfrak{G}$ mit 2 *aufgehen,* und folglich kann statt (23.) auch geschrieben werden:

$$24.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}.2p^e - 1 \quad \text{oder} \quad 25.\quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1.$$

Demnach ist gemäfs (9.)

26. $Z = \mathfrak{S}z + \mathfrak{S}z - 1 = \mathfrak{S}z - 1$ auch für $z = 2p^e$, für jede Stammzahl $p > 2$ und jedes $e > 0$.

M. Nachdem bis hieher von den verschiedenen Zusammensetzungsarten von z (8.) die Fälle

27. $\begin{cases} \mu = 0, & m = 1\ (G.), \quad m = 2\ (H.), \quad m > 2\ (I.) \text{ und} \\ \mu = 1, & m = 0\ (K.), \quad m = 1\ (L.) \end{cases}$

durchgegangen sind, bleiben noch die beiden Fälle

28. $\mu = 1, \quad m > 1$ und

29. $\mu > 1, \quad m$ beliebig

übrig. Sind diese noch untersucht, so sind *alle möglichen* Fälle berührt. Die beiden Fälle (28. und 29.) lassen sich aber wie folgt *zusammenfassen.*

N. *Sechstens.* *a.* Nach (§. 97. II.) giebt es immer, was auch z (8.) sein mag, zu z theilerfremde Zahlen w (dort W), welche zu z (dort Z) und zu den Stammfactoren p_1 von z oder auch zu $p_1^{e_1}$ *zugleich Nichtquadratreste* sind. Sie werden aus den Gleichungen (7. und 8. §. 97. II.) gefunden.

b. Für eine solche Zahl w ist, da sie Nichtquadratrest zu $p_1^{e_1}$ ist, nach (§. 97. 5.),

30. $w^{\frac{1}{2}\varphi p_1^{e_1}} = \mathfrak{S}p_1^{e_1} - 1.$

Da die Zahl w zu z *theilerfremd* ist, so ist sie es auch zu den andern Factoren $p_2^{e_2}, p_3^{e_3}, \dots p_\mu^{e_\mu}$ und 2^m von z (8.), und folglich ist für sie zugleich zufolge (§. 97. 6.), w mag Nichtquadratrest oder Quadratrest zu $p_2^{e_2}, p_3^{e_3}, \dots 2^m$ sein,

31. $\begin{cases} w^{\frac{1}{2}\varphi p_2^{e_2}} = \mathfrak{S}p_2^{e_2} \pm 1, \\ w^{\frac{1}{2}\varphi p_3^{e_3}} = \mathfrak{S}p_3^{e_3} \pm 1, \\ \dots\dots\dots\dots \\ w^{\frac{1}{2}\varphi 2^m} = \mathfrak{S}2^m \pm 1. \end{cases}$

c. Nun ist für z (8.) gemäfs (§. 81. 7.)

32. $\frac{1}{2}\varphi z = \frac{1}{2}.2^{m-1} p_1^{e_1-1}.p_2^{e_2-1}.p_3^{e_3-1}\dots p_\mu^{e_\mu-1}(p_1-1)(p_2-1)(p_3-1)\dots(p_\mu-1)$

und

33. $\begin{cases} \frac{1}{2}\varphi p_1^{e_1} = \frac{1}{2}p_1^{e_1-1}(p_1-1), \\ \frac{1}{2}\varphi p_2^{e_2} = \frac{1}{2}p_2^{e_2-1}(p_2-1), \\ \frac{1}{2}\varphi p_3^{e_3} = \frac{1}{2}p_3^{e_3-1}(p_3-1), \\ \dots\dots\dots\dots \\ \frac{1}{2}\varphi 2^m = \frac{1}{2}.2^{m-1} = 2^{m-2}. \end{cases}$

Aus (32. und 33.) folgt

$$34. \begin{cases} \frac{1}{2}\varphi z = 2^{m-1} p_2^{e_2-1}.p_3^{e_3-1}.p_4^{e_4-1}\dots p_\mu^{e_\mu-1}(p_2-1)(p_3-1)(p_4-1)\dots(p_\mu-1)\times\frac{1}{2}\varphi p_1^{e_1}, \\ \frac{1}{2}\varphi z = 2^{m-1} p_1^{e_1-1}.p_3^{e_3-1}.p_4^{e_4-1}\dots p_\mu^{e_\mu-1}(p_1-1)(p_3-1)(p_4-1)\dots(p_\mu-1)\times\frac{1}{2}\varphi p_2^{e_2}, \\ \frac{1}{2}\varphi z = 2^{m-1} p_1^{e_1-1}.p_2^{e_2-1}.p_4^{e_4-1}\dots p_\mu^{e_\mu-1}(p_1-1)(p_2-1)(p_4-1)\dots(p_\mu-1)\times\frac{1}{2}\varphi p_3^{e_3}, \\ \dots\dots\dots \\ \frac{1}{2}\varphi z = p_1^{e_1-1}.p_2^{e_2-1}.p_3^{e_3-1}\dots p_\mu^{e_\mu-1}(p_1-1)(p_2-1)(p_3-1)\dots(p_\mu-1)\times\frac{1}{2}\varphi 2^m. \end{cases}$$

d. Will man also aus (30. und 31.) wissen, was $w^{\frac{1}{2}\varphi z}$ sei, *worauf es in* (9.) *ankommt,* so mufs man die Gleichungen (30. und 31.), also auch die Gröfsen $\mathfrak{G}p_1^{e_1}-1$, $\mathfrak{G}p_2^{e_2}\pm1$, $\mathfrak{G}p_3^{e_3}\pm1$, ... $\mathfrak{G}2^m\pm1$ rechterhand in denselben, der Reihe nach noch zu Potenzen erheben, deren Exponenten in (34. rechts) diejenigen Producte sind, welche $\frac{1}{2}\varphi p_1^{e_1}$, $\frac{1}{2}\varphi p_2^{e_2}$, $\frac{1}{2}\varphi p_3^{e_3}$, ... $\frac{1}{2}\varphi 2^m$ multipliciren.

e. Diese Producte sind aber in den beiden noch zu untersuchenden Fällen (28. und 29.) immer *gerade* Zahlen. Denn in dem ersten Fall (28.) $\mu=1$, $m>1$ sind jene Producte der Reihe nach 2^{m-1}, 2^{m-1}, 2^{m-1}, ... $p^{e_1-1}(p_1-1)$ und 2^{m-1} ist *gerade,* wenn $m>1$ (28.) ist; desgleichen ist $p^{e_1-1}(p_1-1)$ *gerade,* weil p_1 *ungerade,* also p_1-1 *gerade* ist. Im zweiten Fall (29.), $\mu>1$ und m beliebig, enthalten alle die Producte *wenigstens einen* der Factoren p_1-1, p_2-1, p_3-1, ... $p_\mu-1$, und alle diese Factoren sind *gerade,* weil alle die p nach der Voraussetzung *ungerade* sind.

Es sind demnach die Gröfsen rechterhand in (30. und 31.), um $w^{\frac{1}{2}\varphi z}$ zu finden, sämmtlich zu Potenzen zu erheben, deren Exponenten *gerade* sind, und daher giebt (30. und 31.)

$$35. \begin{cases} w^{\frac{1}{2}\varphi z} = \mathfrak{G}p_1^{e_1}+1, \\ w^{\frac{1}{2}\varphi z} = \mathfrak{G}p_2^{e_2}+1, \\ w^{\frac{1}{2}\varphi z} = \mathfrak{G}p_3^{e_3}+1, \\ \dots\dots\dots \\ w^{\frac{1}{2}\varphi z} = \mathfrak{G}p_\mu^{e_\mu}+1, \\ w^{\frac{1}{2}\varphi z} = \mathfrak{G}2^m+1. \end{cases}$$

f. Aus (35.) folgt nun, dafs $w^{\frac{1}{2}\varphi z}-1$ sowohl mit $p_1^{e_1}$, als mit $p_2^{e_2}$, $p_3^{e_3}$, ... $p_\mu^{e_\mu}$ und 2^m, also mit *allen* Factoren von z (8.) *aufgehen* mufs. Und da alle diese Factoren von z unter sich *theilerfremd* sind, so mufs nach (§. 26.) $w^{\frac{1}{2}\varphi z}-1$ auch mit z *selbst* aufgehen, und folglich $w^{\frac{1}{2}\varphi z}-1=\mathfrak{G}z$ oder

$$36. \quad w^{\frac{1}{2}\varphi z} = \mathfrak{G}z+1 \text{ sein.}$$

Dies in (9.) gesetzt giebt

37. $Z = \mathfrak{G}z + \mathfrak{G}z + 1 = \mathfrak{G}z + 1$ für $\mu = 1$ und $m > 1$, und für $\mu > 1$ und m beliebig (28. und 29.).

O. Zusammen hat sich also in (11. 13. 16. 19. 26. und 37.) gefunden, daſs

38. $Z = \mathfrak{G}z - 1$ ist für $z = 2^2 = 4$ (13.), $z = p^e$ (19.) und $z = 2p^e$ (26.) und in *allen* übrigen Fällen

39. $Z = \mathfrak{G}z + 1$ (11. 16. u. 37.); wie es der Lehrsatz in (1. u. 2.) behauptet.

P. Anmerkung. Der erste Beweis beruht insbesondere auf den Sätzen (§. 92. I., 95. und 96.), der zweite Beweis auf (§. 92. II., 97. und 98.).

§. 100.

Lehrsatz.

Es sei z *eine beliebige ganze Zahl, die also immer durch*

1. $z = 2^m . p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_\mu^{e_\mu}$

ausgedrückt werden kann, wo die sämmtlichen p *Stammzahlen* > 2 *und die* e *beliebige positive ganze Zahlen sind. Die zu* z *theilerfremden Zahlen sollen wie immer durch* z_φ *bezeichnet werden, die Anzahl derjenigen von ihnen, welche* > 0 *und* $<$ z *sind, durch* φz, *die Anzahl der Werthenpaare von* $x < z$, *welche der Gleichung*

2. $x^2 = \mathfrak{G}z + 1$

genugthun, wie oben durch n, *und die Anzahl der verschiedenen zu* z *möglichen Quadratreste durch* ν. *Alsdann ist*

I. *Für jedes* z_φ,

3. $z_\varphi^{\frac{\varphi z}{n}} = \mathfrak{G}z + 1$, *oder auch* 4. $z_\varphi^{2\nu} = \mathfrak{G}z + 1$;

wo nach (§. 81. 7.)

5. $\varphi z = 2^{m-1} . p_1^{e_1 - 1} . p_2^{e_2 - 1} . p_3^{e_3 - 1} \dots p_\mu^{e_\mu - 1} (p_1 - 1)(p_2 - 1)(p_3 - 1) \dots (p_\mu - 1)$,

nach (§. 96.)

6. $\begin{cases} n = 2^{\mu-1} & \textit{für } m = 0 \textit{ und } m = 1, \\ n = 2^\mu & \textit{für } m = 2, \\ n = 2^{\mu+1} & \textit{für } m > 2 \end{cases}$

und nach (§. 94. 4.) 7. $2\nu = \frac{\varphi z}{n}$ *ist.*

Zwar kann schon eine noch niedrigere als die 2ν*te Potenz von* z_φ *zu* z *den Rest* 1 *lassen, aber jedenfalls giebt diese Potenz den Rest* 1 *bis* z.

Dieses ist eine Vereinfachung oder, wenn man will, nähere Bestimmung des verallgemeinerten Fermatschen Satzes (§. 87.); *denn dieser sagt bloſs aus, daſs*

8. $z_\varphi^{\varphi z} = \mathfrak{G}z + 1$,

nicht, daſs schon nach (3.) $z_\varphi^{\frac{\varphi z}{n}} = \mathfrak{G}z + 1$ *ist.*

II. *Eine andere solche Vereinfachung oder nähere Bestimmung des verallgemeinerten Fermatschen Satzes besteht darin, dafs für jedes* $z > 2$, *für welches also* $\frac{1}{2}\varphi z$ *kein Bruch ist und für jede zu einem solchen* z *theilerfremde Zaht* z_φ,

$$9. \quad z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$$

ist, mit alleiniger Ausnahme

10. *der Nichtquadratreste zu* $z = 2^2$, p^e *und* $2p^e$; *welche* $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ *geben.*

III. *Ferner ist zu bemerken, dafs für* $z = 2^2$, p^e *und* $2p^e$ *nur ein einziges Paar der* $z_\varphi > 0$ *und* $< z$ *quadrirt zu* z *den Rest* 1 *läfst, so dafs* $n = 1$ *ist. Hingegen zu allen andern* $z > 2$ *giebt es mehrere und wenigstens 2 solcher Werthenpaare und* n *ist also* > 1.

Beispiel zu I. In dem ersten Beispiel zu (§. 94.) ist $z = 180$, $n = 4$, $\nu = 6$ und $\varphi z = 48$. Eine der zu z theilerfremden Zahlen z_φ ist 77: also soll nach (3.) $77^{\frac{48}{4}} = 77^{12} = \mathfrak{G}.180 + 1$ sein. Es ist, wie aus (§. 94. 23.) zu sehen, $77^2 = \mathfrak{G}z + 169$; 169^2 oder $77^4 = \mathfrak{G}z + 121$; 121^2 oder $77^8 = \mathfrak{G}z + 61$, folglich $77^{12} = 77^8.77^4 = (\mathfrak{G}z + 61)(\mathfrak{G}z + 121) = \mathfrak{G}z + 61.121 = \mathfrak{G}z + 7381 = \mathfrak{G}z + 1$; gemäfs (3.). Jedoch kann auch schon eine *niedrigere* als die $2\nu = 12$te Potenz eines z_φ, $\mathfrak{G}z + 1$ geben. Z. B. $z_\varphi = 53$ giebt nach (§. 94. 23.) $53^2 = \mathfrak{G}z + 109$, und schon $53^4 = \mathfrak{G}z + 109^2$ giebt $\mathfrak{G}z + 1$. Für $z_\varphi = 71$ (§. 94. 23.) ist sogar schon $z_\varphi^2 = \mathfrak{G}z + 1$.

In dem vierten Beispiel zu (§. 94.) ist $z = 120$, $n = 8$, $\nu = 2$ und $\varphi z = 32$. Eine der zu z theilerfremden Zahlen z_φ ist 17; also soll nach (3. und 4.) $17^{\frac{32}{8}} = 17^4 = \mathfrak{G}z + 1 = \mathfrak{G}\,120 + 1$ sein. Es ist $17^2 = 289 = \mathfrak{G}z + 49$ und $17^4 = \mathfrak{G}z + 49^2 = \mathfrak{G}z + 2401 = \mathfrak{G}z + 1$; gemäfs (2.). Aber $z_\varphi = 11$ giebt schon $z_\varphi^2 = 121 = \mathfrak{G}z + 1$.

Zu II. und III. Die z_φ mit ihren Quadratresten r und die φz sind:

11. Für $z = 4$: $z_\varphi = 1, 3$; $r = 1, 1$; $\varphi z = 2$, $\frac{1}{2}\varphi z = 1$;

12. Für $z = 5^2 = 25 = p^e$ $\left\{\begin{array}{l} z_\varphi = 1\;2\;3\;4\;6\;7\;8\;9\;11\;12\;13\;14\;16\;17\;18\;19\;21\;22\;23\;24, \\ r\; = 1\;4\;9\;16\;11\;24\;14\;6\;21\;19\;19\;21\;6\;14\;24\;11\;16\;9\;4\;1, \\ \varphi z = 4.5 = 20, \quad \frac{1}{2}\varphi z = 10; \end{array}\right.$

13. Für $z = 2.3^3 = 18 = 2p^e$ $\left\{\begin{array}{l} z_\varphi = 1\;5\;7\;11\;13\;17, \\ r = 1\;7\;13\;13\;7\;1, \\ \varphi z = 3.2 = 6, \quad \frac{1}{2}\varphi z = 3; \end{array}\right.$

14. Für $z = 2^2.7 = 28 = 2^2 p$ $\left\{\begin{array}{l} z_\varphi = 1\;3\;5\;9\;11\;13\;15\;17\;19\;23\;25\;27, \\ r = 1\;9\;25\;25\;9\;1\;1\;9\;25\;25\;9\;1, \\ \varphi z = 2.6 = 12, \quad \frac{1}{2}\varphi z = 6; \end{array}\right.$

15. Für $z = 2.3.5 = 30 = 2p_1p_2$ $\left\{\begin{array}{l} z_\varphi = 1\;7\;11\;13\;17\;19\;23\;29, \\ r = 1\;19\;1\;19\;19\;1\;19\;1, \\ \varphi z = 2.4 = 8, \quad \frac{1}{2}\varphi z = 4. \end{array}\right.$

Der *Nichtquadratrest* 3 zu $z=4$ (11.) giebt $3^{\frac{1}{2}\varphi z}=3^1=3=\mathfrak{G}z-1$; der *Quadratrest* 1 dagegen giebt $1^{\frac{1}{2}\varphi z}=\mathfrak{G}z+1$; gemäfs (9. und 10.). Ferner ist die Anzahl n der Paare von x, welche $x^2=\mathfrak{G}z+1$ geben, $=1$; gemäfs (III.).

Der *Nichtquadratrest* 7 zu $z=25$ (12.) giebt $7^{\frac{1}{2}\varphi z}=7^{10}=49^5=(\mathfrak{G}z-1)^5=\mathfrak{G}z-1$; der *Quadratrest* 11 dagegen giebt $11^{10}=121^5=(\mathfrak{G}z-4)^5=\mathfrak{G}z-1024=\mathfrak{G}z-(-1)=\mathfrak{G}z+1$; gemäfs (9. und 10.). Die Anzahl n der Paare von x, welche $x^2=\mathfrak{G}z+1$ geben, ist $=1$; gemäfs (III.).

Der *Nichtquadratrest* 5 zu $z=18$ (13.) giebt $5^{\frac{1}{2}\varphi z}=5^3=125=\mathfrak{G}z-1$; der *Quadratrest* 7 dagegen giebt $7^3=343=\mathfrak{G}z+1$; gemäfs (9. und 10.). Die Anzahl n der Paare von x, welche $x^2=\mathfrak{G}z+1$ geben, ist $=1$; gemäfs (III.).

Der *Nichtquadratrest* 3 zu $z=28$ (14.) giebt $3^{\frac{1}{2}\varphi z}=3^6=27^3=(\mathfrak{G}z-1)^2=\mathfrak{G}z+1$ und der *Quadratrest* 9 giebt ebenfalls $9^6=3^{12}=\mathfrak{G}z+1$; gemäfs (9. u. 10.). Die Anzahl n der Paare von x, welche $x^2=\mathfrak{G}z+1$ geben, ist hier $=2$; gemäfs (III.).

Der *Nichtquadratrest* 7 zu $z=30$ (15.) giebt $7^{\frac{1}{2}\varphi z}=7^4=49^2=(\mathfrak{G}z+19)^2=\mathfrak{G}z+361=\mathfrak{G}z+1$ und der *Quadratrest* 19 giebt ebenfalls $19^4=361^2=(\mathfrak{G}z+1)^2=\mathfrak{G}z+1$; gemäfs (9. und 10.). Die Anzahl n der Paare von x, welche $x^2=\mathfrak{G}z+1$ geben, ist hier wieder $=2$; gemäfs (III.).

Beweis von I. *A*. Nach (§. 94. 7.) ist für jeden beliebigen *Quadratrest* r zu z, also für jedes r, welches der Gleichung

16. $z_\varphi^2=\mathfrak{G}z+r$ genugthut,

17. $r^{\frac{\varphi z}{2n}}=\mathfrak{G}z+1$,

oder auch, da nach (§. 94. 4.)

18. $\varphi z=2n\nu$ ist,

19. $r^\nu=\mathfrak{G}z+1$.

B. Nimmt man nun von (16.) die $\frac{\varphi z}{2n}$te oder die νte Potenz, so ergiebt sich

20. $z_\varphi^{\frac{\varphi z}{n}}=\mathfrak{G}z+r^{\frac{\varphi z}{2n}}$ oder 21. $z_\varphi^{2\nu}=\mathfrak{G}z+r^\nu$;

und dieses gilt für *jedes* z_φ. Also ist, wenn man (17. u. 19.) in (18. u. 21.) setzt,

22. $z_\varphi^{\frac{\varphi z}{n}}=\mathfrak{G}z+1$ oder 23. $z_\varphi^{2\nu}=\mathfrak{G}z+1$;

gemäfs (3. und 4.) im Lehrsatz.

Beweis von II. *C*. Die zu z theilerfremden Zahlen z_φ sind entweder *Quadratreste* oder *Nichtquadratreste* zu z.

a. Es bezeichne *Erstlich* r die *Quadratreste* zu den z_φ, so giebt

24. $z_\varphi^2=\mathfrak{G}z+r$

alle Quadratreste r zu z, wenn man z_φ alle seine Werthe durchlaufen läfst. Nimmt man nun von (24.) die $\frac{1}{2}\varphi z$te Potenz, so ergiebt sich

25. $z_\varphi^{2\cdot\frac{1}{2}\varphi z}=z^{\varphi z}=\mathfrak{G}z+r^{\frac{1}{2}\varphi z}$.

Nach dem verallgemeinerten *Fermatschen* Lehrsatze (§. 87.) ist aber für *jedes* z_φ:

26. $z_\varphi^{\varphi z} = \mathfrak{G}z + 1$, also ist in (25.)

27. $\mathfrak{G}z + r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$, und daraus folgt

28. $r^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$:

also ist, erstlich, fur jedes $z_\varphi = r$, welches ein *Quadratrest* zu z ist, *ohne alle Ausnahme*,

29. $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$.

b. Es bezeichne *Zweitens* w die *Nichtquadratreste* zu z_φ, so ist nach (§. 92. 7.)

30. $Z = z_1 z_2 z_3 \ldots . z_{\varphi z} = \mathfrak{G}z + w^{\frac{1}{2}\varphi z}$.

Nun ist nach (§. 99. 1. und 2.)

31. $Z = \mathfrak{G}z - 1$ für $z = 2^2$, p^e und $2p^e$ und

32. $Z = \mathfrak{G}z + 1$ für *jedes* andere z; also ist in (30.)

33. $\mathfrak{G}z + w^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ für $z = 2^2$, p^e und $2p^e$ und

34. $\mathfrak{G}z + w^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$ für *jedes* andere z.

Daraus folgt für die $z_\varphi = w$, welche *Nichtquadratreste* zu z sind,

35. $z^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ für $z = 2^2$, p^e und $2p^e$ und

36. $z^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$ für *jedes* andere z.

c. Es folgt also zusammengenommen aus (29. 35. und 36.), dafs für alle zu z theilerfremden Zahlen z_φ,

37. $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$

ist, mit alleiniger *Ausnahme* der *Nichtquadratreste* zu $z = 2^2$, p^e und $2p^e$, welche nach (35.) $z_\varphi^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ geben; gemäfs II.

Beweis von III. *D. a.* Da nach (3.) für *jedes* z_φ *ohne alle Ausnahme*

38. $z_\varphi^{\frac{\varphi z}{n}} = \mathfrak{G}z + 1$,

nach (35.) aber für die *Nichtquadratreste* zu $z = 2^2$, p^e und p^{2e} *nicht* $z^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$, sondern $z^{\frac{1}{2}\varphi z} = \mathfrak{G}z - 1$ und also erst $z^{\varphi z} = \mathfrak{G}z + 1$ ist, so kann für diese *Nichtquadratreste* zu $z = 2^2$, p^e und $2p^e$ in (38.) n *nicht gröfser* als 1 sein.

b. Für *alle* andern z_φ zu jedem beliebigen z ist dagegen nach (29. u. 36.) $z^{\frac{1}{2}\varphi z} = \mathfrak{G}z + 1$: also ist für *alle* diese z_φ in (38.) n *wenigstens* $= 2$; gemäfs (III.).

Anm. *E.* Diejenigen z_φ, von welchen *keine niedrigere* als die $2\nu = \frac{\varphi z}{n}$te Potenz zu z den Rest 1 läfst, sind für *beliebige* Zahlen z nichts anders als das was für *Stammzahlen* in (§. 57.) *Hauptstammwurzeln* genannt worden ist. Die andern z_φ sind Stammwurzeln für *niedrigere* Exponenten λ als 2ν, wenn jedesmal *keine niedrigere* als die λte Potenz von z_φ zu z den Rest 1 läfst. Hieraus eröffnet sich eine Theorie der Stammwurzeln für *beliebige* Zahlen z, als eine Erweiterung der obigen Theorie (§. 57. etc.) für *Stammzahlen*. Sie bleibt der Folge vorbehalten.

Nachricht für den Buchbinder. ... folgen Tafel I., Tafel II. und Tafel III.

Tafel I.

Sie giebt die Reste r an, welche bleiben, wenn man die 1te, 2te, 3te, ... bis p − 1 = 60te Potenz der Zahlen z = 1, 2, 3, 4, ... 60 (= p − 1) durch die Stammzahl p = 61 dividirt.

In der obersten horizontalen Zeile stehen die Zahlen $z = 1, 2, 3, 4, \ldots\, p-1 = 60$; in der ersten verticalen Reihe links stehen die Exponenten ε der Potenzen dieser Zahlen z, und in den dazu correspondirenden horizontalen Zeilen die Reste r aus

$$z^{\varepsilon} = \mathfrak{G}p + r.$$

Z. B. die Zahlen 1, 54, 41, 49, 46, 18 etc. in der 19ten horizontalen Zeile sind die Reste r der $\varepsilon = 19$ten Potenzen von 1, 2, 3, 4, 5, 6 etc. dividirt durch $p = 61$.

1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
2	1	4	9	16	25	36	49	3	20	39	60	22	47	13	42	12	45	19	56	34	14	57	41	27	15	5	58	52	48	46	46	48	52	58	5	15	27	41	57	14	34	56	19	45	12	42	13	47	22	60	39	20	3	49	36	25	16	9	4	1
3	1	8	27	3	3	33	38	24	58	24	50	20	1	60	20	9	33	37	27	9	50	34	28	38	9	8	41	53	50	38	23	11	8	20	53	52	23	33	27	11	52	34	24	28	52	41	1	60	41	11	37	3	37	23	28	58	58	34	53	60
4	1	16	20	12	15	15	22	9	34	57	1	57	13	47	56	22	12	56	25	58	13	16	34	58	42	25	9	20	47	42	42	47	20	9	25	42	58	34	16	13	58	25	56	12	22	56	47	13	57	1	57	34	9	22	15	15	12	20	16	1
5	1	32	60	48	14	29	32	11	1	21	11	13	47	48	47	47	21	32	48	1	29	47	50	50	13	40	60	11	21	40	21	40	50	1	21	48	11	11	14	32	60	13	29	40	14	14	13	14	48	50	40	60	50	29	32	47	13	1	29	60
6	1	3	58	9	9	52	41	27	9	27	60	34	1	1	34	20	52	27	58	20	50	58	52	41	20	3	34	3	60	41	41	60	3	34	3	20	41	52	58	60	20	58	27	52	20	34	1	1	34	60	27	9	27	41	52	9	9	58	3	1
7	1	6	52	36	45	7	43	33	20	26	50	42	13	14	22	15	30	59	4	34	40	56	37	8	12	17	3	23	32	10	51	29	38	58	44	49	53	24	5	21	27	57	2	31	46	39	47	48	19	11	35	41	28	18	54	16	25	9	55	60
8	1	12	34	22	42	42	57	20	58	16	1	16	47	13	25	57	22	25	15	9	47	12	58	9	56	15	20	34	13	56	56	13	34	20	15	56	9	58	12	47	9	15	25	22	57	25	13	47	16	1	16	58	20	57	42	42	22	34	12	1
9	1	24	41	27	27	8	33	38	34	38	11	9	1	60	9	58	8	23	41	58	11	20	53	33	58	24	52	37	11	33	28	50	24	9	37	3	28	8	41	50	3	20	38	53	3	52	1	60	52	50	23	27	23	28	53	34	34	20	37	60
10	1	48	1	47	13	48	48	60	1	14	60	47	13	47	13	13	14	48	47	1	48	13	60	60	47	14	1	60	14	14	14	14	60	1	14	47	60	60	13	48	1	47	48	14	13	13	47	13	47	60	14	1	60	48	48	13	47	1	48	1
11	1	35	3	5	4	44	31	53	9	18	50	15	47	48	12	25	55	10	39	20	32	42	38	37	16	59	27	33	40	54	7	21	28	34	2	45	24	23	19	29	41	22	51	6	36	49	13	14	46	11	43	52	8	30	17	57	56	58	26	60
12	1	9	9	20	20	20	34	58	20	58	1	58	1	1	58	34	20	58	9	34	1	9	20	34	34	9	58	9	1	34	34	1	9	58	9	34	34	20	9	1	34	9	58	20	34	58	1	1	58	1	58	20	58	34	20	20	20	9	9	1
13	1	18	27	19	39	59	55	37	58	31	11	25	13	14	16	56	35	7	49	9	21	15	33	23	57	51	41	8	29	44	17	32	53	20	10	4	38	28	46	40	52	12	54	26	5	45	46	48	36	50	30	3	24	6	2	22	42	34	43	60
14	1	36	20	15	12	49	19	52	34	5	60	56	47	13	57	42	46	4	16	58	14	25	27	3	22	45	9	41	48	39	39	48	41	9	45	22	3	27	25	14	58	16	4	46	42	57	13	47	56	60	5	34	52	19	49	12	15	20	36	1
15	1	11	60	60	60	50	11	50	1	50	50	1	1	60	1	1	50	11	60	1	50	1	11	11	1	11	60	50	50	11	50	11	11	1	50	60	50	50	60	11	60	1	50	11	60	60	1	60	60	11	11	60	11	60	11	1	1	1	50	60
16	1	22	58	57	36	56	16	34	9	12	1	12	13	47	15	16	57	15	42	20	13	22	9	20	25	42	34	58	47	25	25	47	58	34	42	25	20	9	22	13	20	42	15	57	16	15	47	13	12	1	12	9	34	16	56	56	57	58	22	1
17	1	44	52	45	36	31	51	28	20	59	11	22	47	48	42	2	54	26	5	34	29	57	24	53	15	55	3	38	21	18	43	40	23	58	6	46	8	37	4	32	27	56	35	7	59	19	13	14	39	50	2	41	33	9	30	25	16	9	17	60
18	1	27	34	58	58	3	52	41	58	41	60	20	1	1	20	9	3	41	34	9	60	34	3	52	9	27	20	27	60	52	52	60	27	20	27	9	52	3	34	60	9	34	41	3	9	20	1	1	20	60	41	58	41	52	3	58	58	34	27	1
19	1	54	41	49	46	18	59	23	34	44	50	57	13	14	56	22	51	6	36	58	40	16	8	28	42	31	52	24	32	35	26	29	37	9	30	19	33	53	45	21	3	25	55	10	39	5	47	48	4	11	17	27	38	2	43	15	12	20	7	60
20	1	47	1	13	47	47	47	1	1	13	1	13	47	13	47	47	13	47	13	1	47	47	1	1	13	13	1	1	13	13	13	13	1	1	13	13	1	1	47	47	1	13	47	13	47	47	13	47	13	1	13	1	1	47	47	47	13	1	47	1
21	1	33	3	52	52	38	24	8	9	8	11	34	1	60	34	20	38	53	3	20	11	58	23	24	20	33	27	28	11	24	37	50	33	34	28	41	37	38	3	50	41	58	8	23	41	27	1	60	27	50	53	52	53	37	23	9	9	58	28	60
22	1	5	9	25	16	45	46	3	20	19	60	42	13	47	22	15	36	39	57	34	48	56	41	27	12	4	58	52	14	49	49	14	52	58	4	12	27	41	56	48	34	57	39	36	15	22	47	13	42	60	19	20	3	46	45	16	25	9	5	1
23	1	10	27	39	19	26	17	24	58	7	50	16	47	48	25	57	2	31	46	9	32	12	28	38	56	43	41	53	40	6	55	21	8	20	18	5	23	33	49	29	52	15	30	59	4	36	13	14	45	11	54	3	37	44	35	42	22	34	50	60
24	1	20	20	34	34	34	58	9	34	9	1	9	1	1	9	58	34	9	20	58	1	20	34	58	58	20	9	20	1	58	58	1	20	9	20	58	58	34	20	1	58	20	9	34	58	9	1	1	9	1	9	34	9	58	34	34	34	20	20	1
25	1	40	60	14	48	21	40	11	1	29	11	47	13	14	13	13	29	40	14	1	21	13	50	50	47	32	60	11	29	32	29	32	50	1	29	14	11	11	48	40	60	47	21	32	48	48	47	48	14	50	32	60	50	11	40	13	47	1	21	60
26	1	19	58	56	57	4	36	27	9	46	60	15	47	13	12	25	5	49	22	20	14	42	52	41	16	39	34	3	48	45	45	48	3	34	39	16	41	52	42	14	20	22	49	5	25	12	13	47	15	60	46	9	27	36	4	57	56	58	19	1
27	1	38	52	41	41	24	8	33	20	33	50	58	1	60	58	34	24	28	52	34	50	9	37	8	34	38	3	23	50	8	53	11	38	58	23	27	53	24	52	11	27	9	33	37	27	3	1	60	3	11	28	41	28	53	37	20	20	9	23	60
28	1	15	34	42	22	22	56	20	58	25	1	25	13	47	16	56	42	16	12	9	13	15	58	9	57	12	20	34	47	57	57	47	34	20	12	57	9	58	15	13	9	12	16	42	56	16	47	13	25	1	25	58	20	56	22	22	42	34	15	1
29	1	30	41	46	49	10	26	38	34	6	11	56	47	48	57	42	43	44	45	58	29	25	53	33	22	7	52	37	21	2	59	40	24	9	54	39	28	8	36	32	3	16	17	18	19	4	13	14	5	40	55	27	23	35	51	12	15	20	31	60
30	1	60	1	1	1	60	60	60	1	60	60	1	1	1	1	1	60	60	1	1	60	1	60	60	1	60	1	60	60	60	60	60	60	1	60	1	60	60	1	60	1	1	60	60	1	1	1	1	1	60	60	1	60	60	60	1	1	1	60	1
31	1	59	3	4	5	55	54	53	9	51	50	12	13	14	15	16	44	43	19	20	40	22	38	37	25	35	27	33	32	31	30	29	28	34	26	36	24	23	39	21	41	42	18	17	45	46	47	48	49	11	10	52	8	7	6	56	57	58	2	60
32	1	57	9	16	25	25	12	58	20	22	1	22	47	13	42	2	16	42	56	34	47	57	20	34	15	56	58	9	13	15	15	13	9	58	56	15	34	20	57	47	34	56	42	16	2	42	13	47	22	1	22	20	58	12	25	25	16	9	57	1
33	1	53	27	3	3	28	23	37	58	37	11	20	1	60	20	9	28	24	27	9	11	34	33	23	9	53	41	8	11	23	38	50	53	20	8	52	38	28	27	50	52	34	37	33	52	41	1	60	41	50	24	3	24	38	33	58	58	34	8	60
34	1	45	20	12	15	46	39	52	34	4	60	57	13	47	56	22	49	5	25	58	48	16	27	3	42	36	9	41	14	19	19	14	41	9	36	42	3	27	16	48	58	25	5	49	22	56	47	13	57	60	4	34	52	39	46	15	12	20	45	1
35	1	29	60	48	14	32	29	50	1	40	50	13	47	48	47	47	40	29	48	1	32	47	11	11	13	21	60	50	40	21	40	21	11	1	40	48	50	50	14	29	60	13	32	21	14	14	13	14	48	11	21	60	11	32	29	47	13	1	32	60
36	1	58	58	9	9	9	20	34	9	34	1	34	1	1	34	20	9	34	58	20	1	58	9	20	20	58	34	58	1	20	20	1	58	34	58	20	20	9	58	1	20	58	34	9	20	34	1	1	34	1	34	9	34	20	9	9	9	58	58	1
37	1	55	52	36	45	54	18	28	20	35	11	42	13	14	22	15	31	2	4	34	21	56	24	53	12	44	3	38	29	51	10	32	23	58	17	49	8	37	5	40	27	57	59	30	46	39	47	48	19	50	26	41	33	43	7	16	25	9	6	60
38	1	49	34	22	42	19	4	41	58	45	60	16	47	13	25	57	39	36	15	9	14	12	3	52	56	46	20	27	48	5	5	48	27	20	46	56	52	3	12	14	9	15	36	39	57	25	13	47	16	60	45	58	41	4	19	42	22	34	49	1
39	1	37	41	27	27	53	28	23	34	23	50	9	1	60	9	58	53	38	41	58	50	20	8	28	58	37	52	24	50	28	33	11	37	9	24	3	33	53	41	11	3	20	23	8	3	52	1	60	52	11	38	27	38	33	8	34	34	20	24	60
40	1	13	1	47	13	13	13	1	1	47	1	47	13	47	13	13	47	13	47	1	13	13	1	1	47	47	1	1	47	47	47	47	1	1	47	47	1	1	13	13	1	47	13	47	13	13	47	13	47	1	47	1	1	13	13	13	47	1	13	1
41	1	26	3	5	4	17	30	8	9	43	11	15	47	48	12	25	6	51	39	20	29	42	23	24	16	24	27	28	21	7	54	40	33	34	37	45	37	38	19	32	41	22	10	55	36	49	13	14	46	50	18	52	53	31	44	57	56	58	35	60
42	1	52	9	20	20	41	27	3	20	3	60	58	1	1	58	34	41	3	9	34	60	9	41	27	34	52	58	52	60	27	27	60	52	58	52	34	27	41	9	60	34	9	3	41	34	58	1	1	58	60	3	20	3	27	41	20	20	9	52	1
43	1	43	27	19	39	2	6	24	58	30	50	25	13	14	16	56	26	54	49	9	40	15	28	38	57	10	41	53	32	17	44	29	8	20	51	4	23	33	46	21	52	12	7	35	5	45	47	48	36	11	31	3	37	55	59	22	42	34	18	60
44	1	25	20	15	12	12	42	9	34	56	1	56	47	13	57	42	15	57	16	58	47	25	34	58	22	16	9	20	13	22	22	13	20	9	16	22	58	34	25	47	58	16	57	15	42	57	13	47	56	1	56	34	9	42	12	12	15	20	25	1
45	1	50	60	60	60	11	50	11	1	11	11	1	1	60	1	1	11	50	60	1	11	1	50	50	1	50	60	11	11	50	11	50	50	1	11	60	11	11	60	50	60	1	11	50	60	60	1	60	60	50	50	60	50	11	50	1	1	1	11	60
46	1	39	58	57	56	5	45	27	9	49	60	12	13	47	15	16	4	46	42	20	48	22	52	41	25	19	34	3	14	36	36	14	3	34	19	25	41	52	22	48	20	42	46	4	16	15	47	13	12	60	49	9	27	45	5	56	57	58	39	1
47	1	17	52	45	36	30	10	33	20	2	50	22	47	48	42	2	7	35	5	34	32	57	37	8	15	6	3	23	40	43	18	21	38	58	55	46	53	24	4	29	27	56	26	54	59	19	13	14	39	11	59	41	28	51	31	25	16	9	44	60
48	1	34	34	58	58	58	9	20	58	20	1	20	1	1	20	9	58	20	34	9	1	34	58	9	9	34	20	34	1	9	9	1	34	20	34	9	9	58	34	1	9	34	20	58	9	20	1	1	20	1	20	58	20	9	58	58	58	34	34	1
49	1	7	41	49	46	43	2	38	34	17	11	57	13	14	56	22	10	55	36	58	21	16	53	33	42	30	52	37	29	26	35	32	24	9	31	19	28	8	45	40	3	25	6	51	39	5	47	48	4	50	44	27	23	59	18	15	12	20	54	60
50	1	14	1	13	47	14	14	60	1	48	60	13	47	13	47	47	48	14	13	1	14	47	60	60	13	48	1	60	48	48	48	48	60	1	48	13	60	60	47	14	1	13	14	48	47	47	13	47	13	60	48	1	60	14	14	47	13	1	14	1
51	1	28	3	52	52	23	37	53	9	53	50	34	1	60	34	20	23	8	3	20	50	58	38	37	20	28	27	33	50	37	24	11	28	34	33	41	24	23	3	11	41	58	53	38	41	27	1	60	27	11	8	52	8	24	38	9	9	58	33	60
52	1	56	9	25	16	16	15	58	20	42	1	42	13	47	22	15	25	22	57	34	13	56	20	34	12	57	58	9	47	12	12	47	9	58	57	12	34	20	56	13	34	57	22	25	15	22	47	13	42	1	42	20	58	15	16	16	25	9	56	1
53	1	51	27	39	19	35	44	37	58	54	11	16	47	48	25	57	59	30	46	9	29	12	33	23	56	18	41	8	21	55	6	40	53	20	43	5	38	28	49	32	52	15	31	2	4	36	13	14	45	50	7	3	24	17	26	42	22	34	10	60
54	1	41	20	34	34	27	3	52	34	52	60	9	1	1	9	58	27	52	20	58	60	20	27	3	58	41	9	41	60	3	3	60	41	9	41	58	3	27	20	60	58	20	52	27	58	9	1	1	9	60	52	34	52	3	27	34	34	20	41	1
55	1	21	60	14	48	40	21	50	1	32	50	47	13	14	13	13	32	21	14	1	40	13	11	11	47	29	60	50	32	29	32	29	11	1	32	14	50	50	48	21	60	47	40	29	48	48	47	48	14	11	29	60	11	40	21	13	47	1	40	60
56	1	42	58	56	57	57	25	34	9	15	1	15	47	13	12	25	56	12	22	20	47	42	9	20	16	22	34	58	13	16	16	13	58	34	22	16	20	9	42	47	20	22	12	56	25	12	13	47	15	1	15	9	34	25	57	57	56	58	42	1
57	1	23	52	41	41	37	53	28	20	28	11	58	1	60	58	34	37	33	52	34	11	9	24	53	34	23	3	38	11	53	8	50	23	58	38	27	8	37	52	50	27	9	28	24	27	3	1	60	3	50	33	41	33	8	24	20	20	9	38	60
58	1	46	34	42	22	39	5	41	58	36	60	25	13	47	16	56	19	45	12	9	48	15	3	52	57	49	20	27	14	4	4	14	27	20	49	57	52	3	15	48	9	12	45	19	56	16	47	13	25	60	36	58	41	5	39	22	42	34	46	1
59	1	31	41	46	49	51	35	23	34	55	50	56	47	48	57	42	18	17	45	58	32	25	8	28	22	54	52	24	40	59	2	21	37	9	7	39	33	53	36	29	3	16	44	43	19	4	13	14	5	11	6	27	38	26	10	12	15	20	30	60
60	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Nachricht für den Buchbinder. Die Tafel wird von diesem Blatte nicht abgeschnitten, sondern bleibt an demselben fest und wird am Ende des Bandes eingebunden, so dafs die Tafel wie eine Figurentafel ganz aus dem Buche herausgeschlagen werden kann.

Tafel II.

Selbige giebt die Reste r *an, welche die verschiedenen Potenzen* z^λ *der Zahlen* $z = 1, 2, 3, 4, \ldots p-1$ *lassen, wenn man diese Potenzen durch die Stammzahlen* p *von* $p = 3$ *bis* $p = 101$ *dividirt, also die* r *in* $z^\lambda = \mathfrak{G}p + r$, *nebst den zugehörigen* z; *desgleichen die Hauptstammwurzeln* z_{p-1} *und die Stammwurzeln* z_δ *aus* 1 *zu* p *für jeden Theiler* δ *von* $p-1$. *Von* $p=3$ *bis* $p=29$ *giebt sie die* r *und die* z *für* $\lambda = 2, 3, 4, 5, \ldots p-2$ *an, von* $p=31$ *bis* $p=101$ *aber nur für diejenigen* λ, *welche in* $p-1$ *aufgehende Stammzahlen sind.*

$$\boxed{p = 3} = 4n-1$$

$$z^2 = \mathfrak{G}p + r$$

$$r = 1$$

$$z = {\scriptstyle 1,\,2}$$

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$$\delta = p-1 = 2, \quad z_\delta = 2$$

$$\delta = 1, \quad z_\delta = 1$$

$$\boxed{p = 5} = 4n+1$$

$$z^\lambda = \mathfrak{G}p + r$$

$$r = 1,\ 2,\ 3,\ 4$$

$$\lambda = 3, \quad z = {\scriptstyle 1 \quad 3 \quad 2 \quad 4}$$

$$r = 1, \quad 4$$

$$\lambda = 2, \quad z = {\scriptstyle 1,4 \quad 2,3}$$

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$$\delta = p-1 = 4, \quad z_\delta = 2,\ 3$$

$$\delta = 2, \quad z_\delta = 4$$

$$\delta = 1, \quad z_\delta = 1$$

$$\boxed{p = 7} = 4n - 1$$

$$z^{\lambda} = \mathfrak{G}p + r$$

	$r =$	1,	2,	3,	4,	5,	6
$\lambda = 5,$	$z =$	1	4	5	2	3	6

	$r =$	1,	2,	4
$\lambda = 2,$	$z =$	1, 6	3, 4	2, 5
$\lambda = 4,$	$z =$	1, 6	2, 4	3, 5

	$r =$	1,	6
$\lambda = 3,$	$z =$	1, 2, 4	3, 5, 6

$$z_{\delta}^{\delta} = \mathfrak{G}p + 1$$

$\delta = p - 1 = 6, \quad z_{\delta} = 3, 5$

$\delta = \underline{3}, \quad z_{\delta} = \underline{2}, 4$

$\delta = 2, \quad z_{\delta} = 6$

$\delta = 1, \quad z_{\delta} = 1$

$$\boxed{p = 11} = 4n - 1$$

$$z^{\lambda} = \mathfrak{G}p + r$$

	$r =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$\lambda = 3,$	$z =$	1	7	9	5	3	8	6	2	4	10
$\lambda = 7,$	$z =$	1	8	5	9	4	7	2	6	3	10
$\lambda = 9,$	$z =$	1	6	4	3	9	2	8	7	5	10

	$r =$	1,	3,	4,	5,	9
$\lambda = 2,$	$z =$	1, 10	5, 6	2, 9	4, 7	3, 8
$\lambda = 4,$	$z =$	1, 10	4, 7	3, 8	2, 9	5, 6
$\lambda = 6,$	$z =$	1, 10	3, 8	4, 7	5, 6	2, 9
$\lambda = 8,$	$z =$	1, 10	2, 9	5, 6	3, 8	4, 7

	$r =$	1,	10
$\lambda = 5,$	$z =$	1, 3, 4, 5, 9	2, 6, 7, 8, 10

$$z_{\delta}^{\delta} = \mathfrak{G}p + 1$$

$\delta = p - 1 = 10, \quad z_{\delta} = 2, 6, 7, 8$

$\delta = 5, \quad z_{\delta} = 3, 4, 5, 9$

$\delta = 2, \quad z_{\delta} = 10$

$\delta = 1, \quad z_{\delta} = 1$

$$\boxed{p = 13} = 4n+1$$

$$z^{\lambda} = \mathfrak{G}p + r$$

	$r =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12
$\lambda = 5$,	$z =$	1	6	9	10	5	2	11	8	3	4	7	12
$\lambda = 7$,	$z =$	1	11	3	4	8	7	6	5	9	10	2	12
$\lambda = 11$,	$z =$	1	7	9	10	8	11	2	5	3	4	6	12

	$r =$	1,	3,	4,	9,	10,	12
$\lambda = 2$,	$z =$	1, 12	4, 9	2, 11	3, 10	6, 7	5, 8
$\lambda = 10$,	$z =$	1, 12	3, 10	6, 7	4, 9	2, 11	5, 8

	$r =$	1,	5,	8,	12
$\lambda = 3$,	$z =$	1, 3, 9	7, 8, 11	2, 5, 6	4, 10, 12
$\lambda = 9$,	$z =$	1, 3, 9	2, 5, 6	7, 8, 11	4, 10, 12

	$r =$	1,	3,	9
$\lambda = 4$,	$z =$	1, 5, 8, 12	2, 3, 10, 11	4, 6, 7, 9
$\lambda = 8$,	$z =$	1, 5, 8, 12	4, 6, 7, 9	2, 3, 10, 11

	$r =$	1,	12
$\lambda = 6$,	$z =$	1, 3, 4, 9, 10, 12	2, 5, 6, 7, 8, 11

$$z_{\delta}^{\delta} = \mathfrak{G}p + 1$$

$\delta = p-1 = 12,\quad z_{\delta} = 2,\ 6,\ 7,\ 11$

$\delta = 6,\quad z_{\delta} = 4,\ 10$

$\delta = 4,\quad z_{\delta} = 5,\ 8$

$\delta = 3,\quad z_{\delta} = 3,\ 9$

$\delta = 2,\quad z_{\delta} = 12$

$\delta = 1,\quad z_{\delta} = 1$

$$\boxed{p = 17} = 4n + 1$$

$$z^\lambda = \mathfrak{G}p + r$$

	r =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
λ = 3,	z =	1	8	7	13	11	5	14	2	15	3	12	6	4	10	9	16
λ = 5,	z =	1	15	12	4	3	10	6	9	8	11	7	14	13	5	2	16
λ = 7,	z =	1	9	11	13	10	14	12	15	2	5	3	7	4	6	8	16
λ = 9,	z =	1	2	14	4	12	11	10	8	9	7	6	5	13	3	15	16
λ = 11,	z =	1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16
λ = 13,	z =	1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16
λ = 15,	z =	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16

	r =	1	2	4	8	9	13	15	16
λ = 2,	z =	1, 16	6, 11	2, 15	5, 12	3, 14	8, 9	7, 10	4, 13
λ = 6,	z =	1, 16	5, 12	8, 9	6, 11	7, 10	2, 15	3, 14	4, 13
λ = 10,	z =	1, 16	7, 10	2, 15	3, 14	5, 12	8, 9	6, 11	4, 13
λ = 14,	z =	1, 16	3, 14	8, 9	7, 10	6, 11	2, 15	5, 12	4, 13

	r =	1	4	13	16
λ = 4,	z =	1, 4, 13, 16	6, 7, 10, 11	3, 5, 12, 14	2, 8, 9, 15
λ = 12,	z =	1, 4, 13, 16	3, 5, 12, 14	6, 7, 10, 11	2, 8, 9, 15

	r =	1	16
λ = 8,	z =	1, 2, 4, 8, 9, 13, 15, 16	3, 5, 6, 7, 10, 11, 12, 14

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 16, \quad z_\delta = 3, 5, 6, 7, 10, 11, 12, 14$

$\delta = 8, \quad z_\delta = 2, 8, 9, 15$

$\delta = 4, \quad z_\delta = 4, 13$

$\delta = 2, \quad z_\delta = 16$

$\delta = 1, \quad z_\delta = 1$

$\boxed{p = 19} = 4n - 1$

$$z^{\lambda} = \mathfrak{G}p + r$$

	$r =$ 1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18
$\lambda = 5,$	$z =$ 1	15	10	16	6	17	11	12	5	14	7	8	2	13	3	9	4	18
$\lambda = 7,$	$z =$ 1	3	14	9	17	4	7	8	6	13	11	12	15	2	10	5	16	18
$\lambda = 11,$	$z =$ 1	13	15	17	9	5	11	12	16	3	7	8	14	10	2	4	6	18
$\lambda = 13,$	$z =$ 1	14	2	6	16	9	7	8	4	15	11	12	10	3	13	17	5	18
$\lambda = 17,$	$z =$ 1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18

	$r =$ 1,	4,	5,	6,	7,	9,	11,	16,	17
$\lambda = 2,$	$z =$ 1, 18	2, 17	9, 10	5, 14	8, 11	3, 16	7, 12	4, 15	6, 13
$\lambda = 4,$	$z =$ 1, 18	6, 13	3, 16	9, 10	7, 12	4, 15	8, 11	2, 17	5, 14
$\lambda = 8,$	$z =$ 1, 18	5, 14	4, 15	3, 16	8, 11	2, 17	7, 12	6, 13	9, 10
$\lambda = 10,$	$z =$ 1, 18	4, 15	5, 14	6, 13	7, 12	9, 10	8, 11	3, 16	2, 17
$\lambda = 14,$	$z =$ 1, 18	3, 16	6, 13	2, 17	8, 11	5, 14	7, 12	9, 10	4, 15
$\lambda = 16,$	$z =$ 1, 18	9, 10	2, 17	4, 15	7, 12	6, 13	8, 11	9, 14	3, 16

	$r =$ 1,	7,	8,	11,	12,	18
$\lambda = 3,$	$z =$ 1, 7, 11	4, 6, 9	2, 3, 14	5, 16, 17	10, 13, 15	8, 12, 18
$\lambda = 15,$	$z =$ 1, 7, 11	5, 16, 17	10, 13, 15	4, 6, 9	2, 3, 14	8, 12, 18

	$r =$ 1,	7,	11
$\lambda = 6,$	$z =$ 1, 7, 8, 11, 12, 18	2, 3, 5, 14, 16, 17	4, 6, 9, 10, 13, 15
$\lambda = 12,$	$z =$ 1, 7, 8, 11, 12, 18	4, 6, 9, 10, 13, 15	2, 3, 5, 14, 16, 17

	$r =$ 1,	18
$\lambda = 9,$ (4)	$z =$ 2, 3, 8, 10, 12, 13, 14, 15, 18	1, 4, 5, 6, 7, 9, 11, 16, 17

| Falsch. die z Reihen zu vertauschen

$$z_{\delta}^{\delta} = \mathfrak{G}p + 1$$

$\delta = p - 1 = 18, \quad z_{\delta} = 2, 3, 10, 13, 14, 15$

$\delta = 9, \quad z_{\delta} = 4, 5, 6, 9, 16, 17$

$\delta = 6, \quad z_{\delta} = 8, 12$

$\delta = 3, \quad z_{\delta} = 7, 11$

$\delta = 2, \quad z_{\delta} = 18$

$\delta = 1, \quad z_{\delta} = 1$

$$\boxed{p = 23} = 4n - 1$$

$$z^{\lambda} = \mathfrak{G}p + r$$

	r = 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
λ = 3, z =	1	16	12	3	19	8	14	2	6	5	10	13	18	17	21	9	15	4	20	11	7	22
λ = 5, z =	1	6	18	13	11	16	15	9	2	20	19	4	13	21	14	8	7	12	10	5	17	22
λ = 7, z =	1	3	6	9	7	18	11	4	13	21	15	8	2	10	19	12	5	16	14	17	20	22
λ = 9, z =	1	9	13	12	20	2	17	16	8	19	6	18	4	15	7	6	21	3	11	10	14	22
λ = 13, z =	1	18	16	2	15	12	19	13	3	17	14	9	6	20	10	4	11	8	21	7	5	22
λ = 15, z =	1	8	4	18	10	9	21	6	16	11	20	3	12	7	17	2	14	13	5	19	15	22
λ = 17, z =	1	4	9	16	21	13	20	18	12	15	17	6	8	11	5	3	10	2	7	14	19	22
λ = 19, z =	1	13	2	8	17	3	5	12	4	14	7	16	9	19	11	18	20	6	15	21	10	22
λ = 21, z =	1	12	8	6	14	4	10	3	18	7	21	2	16	5	20	13	19	9	17	15	11	22

	r = 1	2	3	4	6	8	9	12	13	16	18
λ = 2, z =	1, 22	5, 18	7, 16	2, 21	11, 12	10, 13	3, 20	9, 14	6, 17	4, 19	8, 15
λ = 4, z =	1, 22	8, 15	4, 19	5, 18	9, 14	6, 17	7, 16	3, 20	11, 12	2, 21	10, 13
λ = 6, z =	1, 22	4, 19	9, 14	7, 16	10, 13	5, 18	11, 12	6, 17	8, 15	3, 20	2, 21
λ = 8, z =	1, 22	10, 13	2, 21	8, 15	3, 20	11, 12	4, 19	7, 16	9, 14	5, 18	6, 17
λ = 10, z =	1, 22	11, 12	8, 15	6, 17	4, 19	3, 20	5, 18	2, 21	7, 16	10, 13	9, 14
λ = 12, z =	1, 22	2, 21	3, 20	4, 19	6, 17	8, 15	9, 14	11, 12	10, 13	7, 16	5, 18
λ = 14, z =	1, 22	4, 19	11, 12	3, 20	8, 15	2, 21	6, 17	10, 13	5, 18	9, 14	4, 19
λ = 16, z =	1, 22	6, 17	5, 18	10, 13	7, 16	9, 14	2, 21	4, 19	3, 20	8, 15	11, 12
λ = 18, z =	1, 22	3, 20	6, 17	9, 14	5, 18	4, 19	10, 13	8, 15	2, 21	11, 12	7, 16
λ = 20, z =	1, 22	9, 14	10, 13	11, 12	2, 21	7, 16	8, 15	5, 18	4, 19	6, 17	3, 20

	r = 1	22
λ = 11, z =	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18	5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22

$$z_{\delta}^{\delta} = \mathfrak{G}p + 1$$

$\delta = p - 1 = 22,\quad z_{\delta} = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$

$\delta = 11,\quad z_{\delta} = 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$

$\delta = 2,\quad z_{\delta} = 22$

$\delta = 1,\quad z_{\delta} = 1$

$$\boxed{p = 29} = 4n + 1$$

$$z^\lambda = \mathfrak{G}p + r$$

	r =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\lambda = 3$,	$z =$	1	26	18	9	22	4	16	2	5	21	15	17	6	10	19	23	12	14	8	24	27	13	25	7	20	11	3	28
$\lambda = 5$,	$z =$	1	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14	25	19	5	16	20	23	27	8	28
$\lambda = 9$,	$z =$	1	11	14	5	13	9	23	26	22	27	19	12	4	21	8	25	17	10	2	7	3	6	20	16	24	15	18	28
$\lambda = 11$,	$z =$	1	10	8	13	4	22	20	14	6	11	27	17	5	26	3	24	12	2	18	23	15	9	7	25	16	21	19	28
$\lambda = 13$,	$z =$	1	14	19	22	6	5	25	18	13	26	21	12	9	2	27	20	17	8	3	16	11	4	24	23	7	10	15	28
$\lambda = 15$,	$z =$	1	27	26	4	5	6	7	21	9	19	18	17	13	15	14	16	12	11	10	20	8	22	23	24	25	3	2	28
$\lambda = 17$,	$z =$	1	3	11	9	22	4	16	27	5	8	14	12	6	19	10	23	17	15	21	24	2	13	25	7	20	18	26	28
$\lambda = 19$,	$z =$	1	8	27	6	9	13	24	19	4	14	26	17	22	18	11	7	12	3	15	25	10	5	16	20	23	2	21	28
$\lambda = 23$,	$z =$	1	18	15	5	13	9	23	3	22	2	10	17	4	8	21	25	12	19	27	7	26	6	20	16	24	14	11	28
$\lambda = 25$,	$z =$	1	19	21	13	4	22	20	15	6	18	2	12	5	3	26	24	17	27	11	23	14	9	7	25	16	8	10	28
$\lambda = 27$,	$z =$	1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

	r =	1,	4,	5,	6,	7,	9,	13,	16,	20,	22,	23,	24,	25,	28
$\lambda = 2$,	$z =$	1, 28	2, 27	11, 18	8, 21	6, 23	3, 26	10, 19	4, 25	7, 22	14, 15	9, 20	13, 16	5, 24	12, 17
$\lambda = 6$,	$z =$	1, 28	3, 26	14, 15	2, 27	4, 25	11, 18	8, 21	9, 20	13, 16	10, 19	5, 24	6, 23	7, 22	12, 17
$\lambda = 10$,	$z =$	1, 28	8, 21	3, 26	10, 19	13, 16	2, 27	14, 15	6, 23	5, 24	11, 18	4, 25	7, 22	9, 20	12, 17
$\lambda = 18$,	$z =$	1, 28	11, 18	10, 19	3, 26	9, 20	14, 15	2, 27	5, 24	6, 23	8, 21	7, 22	4, 25	13, 16	12, 17
$\lambda = 22$,	$z =$	1, 28	10, 19	2, 27	14, 15	7, 22	8, 21	11, 18	13, 16	9, 10	3, 26	6, 23	5, 24	4, 25	12, 17
$\lambda = 26$,	$z =$	1, 28	14, 15	8, 21	11, 18	5, 24	10, 19	3, 26	7, 22	4, 25	2, 27	13, 16	9, 20	6, 23	12, 17

	r =	1,	7,	16,	20,	23,	24
$\lambda = 4$,	$z =$	1, 12, 17, 28	8, 9, 20, 21	2, 5, 24, 27	6, 14, 15, 23	3, 7, 22, 26	4, 10, 19, 25
$\lambda = 8$,	$z =$	1, 12, 17, 28	3, 7, 22, 26	11, 13, 16, 18	8, 9, 20, 21	6, 14, 15, 23	2, 5, 24, 27
$\lambda = 12$,	$z =$	1, 12, 17, 28	2, 5, 24, 27	3, 7, 22, 26	4, 10, 19, 25	11, 13, 16, 18	8, 9, 20, 21
$\lambda = 16$,	$z =$	1, 12, 17, 28	6, 14, 15, 23	4, 10, 19, 25	3, 7, 22, 26	8, 9, 20, 21	11, 13, 16, 18
$\lambda = 20$,	$z =$	1, 12, 17, 28	4, 10, 19, 25	8, 9, 20, 21	11, 13, 16, 18	2, 5, 24, 27	6, 14, 15, 23
$\lambda = 24$,	$z =$	1, 12, 17, 28	11, 13, 16, 18	6, 14, 15, 23	2, 5, 24, 27	5, 10, 19, 25	3, 7, 22, 26

	r =	1,	12,	17,	28
$\lambda = 7$,	$z =$	1, 7, 16, 20, 23, 24, 25	2, 3, 11, 14, 17, 19, 21	8, 10, 12, 15, 18, 26, 27	4, 5, 6, 9, 13, 22, 28
$\lambda = 21$,	$z =$	1, 7, 16, 20, 23, 24, 25	8, 10, 12, 15, 18, 26, 27	2, 3, 11, 14, 17, 19, 21	4, 5, 6, 9, 13, 22, 28

	r =	1,	28
$\lambda = 14$,	$z =$	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 28,\quad z_\delta = 2,\ 3,\ 8,\ 10,\ 11,\ 14,\ 15,\ 18,\ 19,\ 21,\ 26,\ 27$

$\delta = 14,\quad z_\delta = 4,\ 5,\ 6,\ 9,\ 13,\ 22$

$\delta = 7,\quad z_\delta = 7,\ 16,\ 20,\ 23,\ 24,\ 25$

$\delta = 4,\quad z_\delta = 12,\ 17$

$\delta = 2,\quad z_\delta = 28$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 31} = 4n - 1$

$$z^2 = \mathfrak{S}p + r$$

$r =$	1,	2,	4,	5,	7,	8,	9,	10,	14,	16,	18,	19,	20,	25,	28
$z =$	1, 30	8, 23	2, 29	6, 25	10, 21	15, 16	3, 28	14, 17	13, 18	4, 27	7, 24	9, 22	12, 19	5, 26	11, 20

$$z^3 = \mathfrak{S}p + r$$

$r =$	1,	2,	4,	8,	15,	16,	23,	27,	29,	30
$z =$	1, 5, 25	4, 7, 20	16, 18, 28	2, 10, 19	17, 22, 23	8, 9, 14	12, 21, 29	3, 13, 15	11, 24, 27	6, 26, 30

$$z^5 = \mathfrak{S}p + r$$

$r =$	1,	5,	6,	25,	26,	30
$z =$	1, 2, 4, 8, 16	7, 14, 19, 25, 28	11, 13, 21, 22, 26	5, 9, 10, 18, 20	3, 6, 12, 17, 24	15, 23, 27, 29, 30

$$z_\delta^\delta = \mathfrak{S}p + 1$$

$\delta = p - 1 = 30, \quad z_\delta = 3, 11, 12, 13, 17, 21, 22, 24$
$\delta = 15, \quad z_\delta = 7, 9, 10, 14, 18, 19, 20, 28$
$\delta = 10, \quad z_\delta = 15, 23, 27, 29$
$\delta = 6, \quad z_\delta = 6, 26$
$\delta = 5, \quad z_\delta = 2, 4, 8, 16$
$\delta = 3, \quad z_\delta = 5, 25$
$\delta = 2, \quad z_\delta = 30$
$\delta = 1, \quad z_\delta = 1$

$\boxed{p = 37} = 4n + 1$

$$z^2 = \mathfrak{S}p + r$$

$r =$	1,	3,	4,	7,	9,	10,	11,	12,	16,	21,	25,	26,	27,	28,	30,	33,	34,	36
$z =$	1, 36	15, 22	2, 35	9, 28	3, 34	11, 26	14, 23	7, 30	4, 33	13, 24	5, 32	10, 27	8, 29	18, 19	17, 20	12, 25	16, 21	6, 31

$$z^3 = \mathfrak{S}p + r$$

$r =$	1,	6,	8,	10,	11,	14,	23,	26,	27,	29,	31,	36
$z =$	1, 10, 26	14, 29, 31	2, 15, 20	7, 33, 34	21, 25, 28	5, 13, 19	18, 24, 32	9, 12, 16	3, 4, 30	17, 22, 35	6, 8, 23	11, 27, 36

$$z_\delta^\delta = \mathfrak{S}p + 1$$

$\delta = p - 1 = 36, \quad z_\delta = 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35$
$\delta = 18, \quad z_\delta = 3, 4, 21, 25, 28, 30$
$\delta = 12, \quad z_\delta = 8, 14, 23, 29$
$\delta = 9, \quad z_\delta = 7, 9, 12, 16, 33, 34$
$\delta = 6, \quad z_\delta = 11, 27$
$\delta = 4, \quad z_\delta = 6, 31$
$\delta = 3, \quad z_\delta = 10, 26$
$\delta = 2, \quad z_\delta = 36$
$\delta = 1, \quad z_\delta = 1$

$\boxed{p = 41} = 4n + 1$

$z^2 = \mathfrak{S}p + r$

$r =$	1	2	4	5	8	9	10	16	18	20	21	23	25	31	32	33	36	37	39	40
$z =$	1, 40	17, 24	2, 39	13, 28	7, 34	3, 38	16, 25	4, 37	10, 31	15, 26	12, 29	8, 33	5, 36	20, 21	14, 27	19, 22	6, 35	18, 23	11, 30	9, 32

$z^5 = \mathfrak{S}p + r$

$r =$	1	3	9	14	27	32	38	40
$z =$	1, 10, 16, 18, 37	11, 12, 28, 34, 38	5, 8, 9, 21, 39	15, 22, 24, 27, 35	6, 14, 17, 19, 26	2, 20, 32, 33, 36	3, 7, 13, 29, 30	4, 23, 25, 31, 40

$z_\delta^\delta = \mathfrak{S}p + 1$

$\delta = p - 1 = 40,\quad z_\delta = 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35$

$\delta = 20,\quad z_\delta = \underline{2}, 5, 8, 20, 21, 33, 36, 39$

$\delta = 1\underline{0},\quad z_\delta = \underline{4}, 23, 25, 31$

$\delta = 8,\quad z_\delta = 3, 14, 27, 38$

$\delta = \underline{5},\quad z_\delta = 10, 16, 18, 37$

$\delta = 4,\quad z_\delta = 9, 32$

$\delta = 2,\quad z_\delta = 40$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 43} = 4n - 1$

$z^2 = \mathfrak{S}p + r$

$r =$	1	4	6	9	10	11	13	14	15	16	17	21	23	24	25	31	35	36	38	40	41
$z =$	1, 42	2, 41	7, 36	3, 40	15, 28	21, 22	20, 23	10, 33	12, 31	4, 39	19, 24	8, 35	18, 25	14, 29	5, 38	17, 26	11, 32	6, 37	9, 34	13, 30	16, 27

$z^3 = \mathfrak{S}p + r$

$r =$	1	2	4	8	11	16	21	22	27	32	35	39	41	42
$z =$	1, 6, 36	20, 32, 34	13, 35, 38	2, 12, 29	10, 16, 17	21, 25, 40	4, 15, 24	19, 28, 39	3, 18, 22	26, 27, 33	14, 31, 41	5, 8, 30	9, 11, 23	7, 37, 42

$z^7 = \mathfrak{S}p + r$

$r =$	1	6	7	36	37	42
$z =$	1, 4, 11, 16, 21, 35, 41	6, 10, 23, 24, 31, 38, 40	7, 18, 26, 28, 29, 30, 34	9, 13, 14, 15, 17, 25, 36	3, 5, 12, 19, 20, 33, 37	2, 8, 22, 27, 32, 39, 42

$z_\delta^\delta = \mathfrak{S}p + 1$

$\delta = p - 1 = 42,\quad z_\delta = 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34$

$\delta = 21,\quad z_\delta = 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40$

$\delta = 14,\quad z_\delta = 2, 8, 22, 27, 32, 39$

$\delta = 7,\quad z_\delta = 4, 11, 16, 21, 35, 41$

$\delta = \underline{6},\quad z_\delta = \underline{7}, 37$

$\delta = 3,\quad z_\delta = 6, 36$

$\delta = 2,\quad z_\delta = 42$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 47} = 4n - 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1	2	3	4	6	7	8	9	12	14	16	17	18	21	24	25	27	28	32	34	36	37	42
$z =$	1	7	12	2	10	17	14	3	23	22	4	8	21	16	20	5	11	13	19	9	6	15	18
	46	40	35	45	37	30	33	44	24	25	43	39	26	31	27	42	36	34	28	38	41	32	29

$$z^{23} = \mathfrak{G}p + r$$

$r =$	1,	46
$z =$	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 46,$ $z_\delta = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45$

$\delta = 23,$ $z_\delta = 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42$

$\delta = 2,$ $z_\delta = 46$

$\delta = 1,$ $z_\delta = 1$

$\boxed{p = 53} = 4n + 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1	4	6	7	9	10	11	13	15	16	17	24	25	28	29	36	37	38	40	42	43	44	46	47	49	52
$z =$	1	2	18	22	3	13	8	15	11	4	21	17	5	9	20	6	14	12	26	25	19	16	24	10	7	23
	52	51	35	31	50	40	45	38	42	49	32	36	48	44	33	47	39	41	27	28	34	37	29	43	46	30

$$z^{13} = \mathfrak{G}p + r$$

$r =$	1,	23,	30,	52
$z =$	1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49	5, 8, 12, 14, 18, 21, 22, 23, 27, 33, 34, 50, 51	2, 3, 19, 20, 26, 30, 31, 32, 35, 39, 41, 45, 48	4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43, 52

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 52,$ $z_\delta = 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51$

$\delta = 26,$ $z_\delta = 4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43$

$\delta = 13,$ $z_\delta = 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49$

$\delta = 4,$ $z_\delta = 23, 30$

$\delta = 2,$ $z_\delta = 52$

$\delta = 1,$ $z_\delta = 1$

$\boxed{p = 59} = 4n - 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1,	3,	4,	5,	7,	9,	12,	15,	16,	17,	19,	20,	21,	22,	25
$z =$	1 58	11 48	2 57	8 51	19 40	3 56	22 37	29 30	4 55	28 31	14 45	16 43	27 32	9 50	5 54
$r =$	26,	27,	28,	29,	35,	36,	41,	45,	46,	48,	49,	51,	53,	57	
$z =$	12 47	26 33	21 38	18 41	25 34	6 53	10 49	24 35	20 39	15 44	7 52	13 46	17 42	23 36	

$$z^{29} = \mathfrak{G}p + r$$

$r =$	1,	58
$z =$	1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57,	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56, 58

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 58,\quad z_\delta = 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56$

$\delta = 29,\quad z_\delta = 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57$

$\delta = 2,\quad z_\delta = 58$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 61} = 4n + 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1,	3,	4,	5,	9,	12,	13,	14,	15,	16,	19,	20,	22,	25,	27
$z =$	1 60	8 53	2 59	26 35	3 58	16 45	14 47	21 40	25 36	4 57	18 43	9 52	12 49	5 56	24 37
$r =$	34,	36,	39,	41,	42,	45,	46,	47,	48,	49,	52,	56,	57,	58,	60
$z =$	20 41	6 55	10 51	23 38	15 46	17 44	30 31	13 48	29 32	7 54	28 33	19 42	22 39	27 34	11 50

$$z^3 = \mathfrak{G}p + r$$

$r =$	1,	3,	8,	9,	11,	20,	23,	24,	27,	28
$z =$	1, 13, 47	4, 5, 52	2, 26, 33	16, 20, 25	32, 40, 50	12, 15, 34	31, 37, 54	8, 10, 43	3, 19, 39	23, 44, 55
$r =$	33,	34,	37,	38,	41,	50,	52,	53,	58,	60,
$z =$	6, 17, 38	22, 42, 58	18, 51, 53	7, 24, 30	27, 46, 49	11, 21, 29	36, 41, 45	28, 35, 59	9, 56, 57	14, 48, 60

$$z^5 = \mathfrak{G}p + r$$

$r =$	1,	11,	13,	14,	21,	29,	32,	40,	47,	48,	50,	60
$z =$	1,9,20 34, 58	8,11,28 37,38	12,25,42 47, 57	5,39,45 46,48	10,17,29 31, 35	6,21,43 54, 59	5, 7, 18 40, 55	24,26,30 32, 51	13,15,16 22, 56	4,14,19 36, 49	23,24,33 50, 53	3,27,41 52, 60

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 60,\quad z_\delta = 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59$

$\delta = 30,\quad z_\delta = 4, 5, 19, 36, 39, 45, 46, 49$

$\delta = 20,\quad z_\delta = 8, 23, 24, 28, 33, 37, 38, 53$

$\delta = 15,\quad z_\delta = 12, 15, 16, 22, 25, 42, 56, 57$

$\delta = 12,\quad z_\delta = 21, 29, 32, 40$

$\delta = 10,\quad z_\delta = 3, 27, 41, 52$

$\delta = 6,\quad z_\delta = 14, 48$

$\delta = 5,\quad z_\delta = 9, 20, 34, 58$

$\delta = 4,\quad z_\delta = 11, 50$

$\delta = 3,\quad z_\delta = 13, 47$

$\delta = 2,\quad z_\delta = 60$

$\delta = 1,\quad z_\delta = 1$

$$\boxed{p = 67} = 4n - 1$$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1,	4,	6,	9,	10,	14,	15,	16,	17,	19,	21,	22,	23,	24,	25,	26
$z =$	1	2	26	3	12	9	22	4	33	32	17	25	31	15	5	19
	66	65	41	64	55	58	45	63	34	35	50	42	36	52	62	48

$r =$	29,	33,	35,	36,	37,	39,	40,	47,	49,	54,	55,	56,	59,	60,	62,	64,	65
$z =$	30	10	13	6	29	21	24	28	7	11	16	18	27	23	14	8	20
	37	57	54	61	38	46	43	39	60	56	51	49	40	44	53	59	47

$$z^3 = \mathfrak{G}p + r$$

$r =$	1,	3,	5,	8,	9,	14,	15,	22,	24,	25,	27.
$z =$	1, 29	18, 53,	32, 45	2, 7	16, 56	25, 54	6, 21	24, 26	36, 39	15, 19	3, 20
	37	63	57	58	62	55	40	42	59	33	44

$r =$	40,	42,	43,	45,	52,	53,	58,	59,	62,	64,	66
$z =$	23, 47	34, 48	8, 28	41, 43	27, 46	12, 13	5, 11	9, 60	10, 22	4, 14	30, 38
	64	52	31	50	61	42	51	65	35	49	66

$$z^{11} = \mathfrak{G}p + r$$

$r =$	1,	29,	30,	37,	38,	66
$z =$	1, 9, 14, 15, 22, 24	6, 10, 16, 17, 19, 23	7, 11, 12, 20, 31, 32	4, 21, 26, 29, 33, 35	2, 13, 18, 28, 30, 44	3, 5, 8, 27, 42, 43
	25, 40, 59, 62, 64	37, 39, 49, 54, 65	34, 38, 41, 46, 63	36, 47, 55, 56, 60	48, 50, 51, 57, 61	45, 52, 53, 58, 66

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 66$, $z_\delta =$ 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63

$\delta = 33$, $z_\delta =$ 4, 6, 10, 16, 17, 19, 21, 23, 26, 33, 35, 36, 39, 47, 49, 54, 55, 56, 60, 65

$\delta = 22$, $z_\delta =$ 3, 5, 8, 27, 42, 43, 45, 52, 53, 58

$\delta = 11$, $z_\delta =$ 9, 14, 24, 25, 40, 59, 62, 64

$\delta = 6$, $z_\delta =$ 15, 22, 30, 38

$\delta = 3$, $z_\delta =$ 29, 37

$\delta = 2$, $z_\delta =$ 66

$\delta = 1$, $z_\delta =$ 1

$$\boxed{p = 71} = 4n - 1$$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1,	2,	3,	4,	5,	6,	8,	9,	10,	12,	15,	16,	18,	19,	20,	24,	25,	27
$z =$	1	12	28	2	17	19	24	3	9	15	21	4	35	27	34	33	5	13
	70	59	43	69	54	52	47	68	62	56	50	67	36	44	37	38	66	58

$r =$	29,	30,	32,	36,	37,	38,	40,	43,	45,	48,	49,	50,	54,	57,	58,	60,	64
$z =$	10	32	23	6	26	31	18	16	20	30	7	11	14	25	22	29	8
	61	39	48	65	45	40	53	55	51	41	64	60	57	46	49	42	63

$$z^5 = \mathfrak{G}p + r$$

$r =$	1,	20,	23,	26,	30,	32,	34,	37,	39,	41,	45,	48,	51,	70
$z =$	1,5,25	27,36,38	11,26,55	22,39,47	3,4,15	2,10,37	13,31,41	6,8,30	21,28,34	42,41,56	18,19,24	9,12,16	7,23,33	14,17,46
	54,57	48,64	59,62	52,53	20,29	43,50	63,65	40,58	61,69	67,68	32,49	45,60	35,44	66,70

$$z^7 = \mathfrak{G}p + r$$

$r =$	1,	5,	14,	17,	25,	46,	54,	57,	66,	70
$z =$	1,20,30,32	10,15,16,24	7,11,31,46	14,21,22,33	5,8,12,18	28,42,44,53	4,6,9,38	2,3,19,25	13,17,35,47	23,26,34,39
	37,45,48	36,54,58	52,68,69	62,65,67	27,29,43	59,63,66	49,50,57	40,60,64	55,56,61	41,51,70

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 70$, $z_\delta =$ 7,11,13,21,22,28,31,33,35,42,44,47,52,53,55,56,59,61,62,63,65,67,68,69

$\delta = 35$, $z_\delta =$ 2, 3, 4, 6, 8, 9,10,12,15,16,18,19,24,27,29,36,38,40,43,49,50,58,60,64

$\delta = 14$, $z_\delta =$ 23,26,34,39,41,51

$\delta = 10$, $z_\delta =$ 14,17,46,66

$\delta = 7$, $z_\delta =$ 20,30,32,37,45,48

$\delta = 5$, $z_\delta =$ 5,25,54,57

$\delta = 2$, $z_\delta =$ 70

$\delta = 1$, $z_\delta =$ 1

$\boxed{p = 73} = 4n+1$

$$z^2 = \mathfrak{G}p + r$$

r =	1	2	3	4	6	8	9	12	16	18	19	23	24	25	27	32	35	36	37	38	41	46	48	49
z =	1	32	21	2	15	9	3	31	4	23	26	13	30	5	10	18	20	6	16	29	25	22	11	7
	72	41	52	71	58	64	70	42	69	50	47	60	43	68	63	55	53	67	57	44	48	51	62	66

r =	50	54	55	57	61	64	65	67	69	70	71	72
z =	14	28	36	35	34	8	24	33	19	17	12	27
	59	45	37	38	39	65	49	40	54	56	61	46

$$z^3 = \mathfrak{G}p + r$$

r =	1	3	7	8	9	10	17	21	22	24	27	30
z =	1, 8	25, 54	13, 29	2, 16	36, 41	43, 51	11, 15	33, 45	17, 63	35, 50	3, 24	34, 53
	64	67	31	55	69	52	47	68	66	61	46	59

r =	43	46	49	51	52	56	63	64	65	66	70	72
z =	14, 20	27, 49	12, 23	7, 10	5, 28	26, 58	21, 22	4, 32	18, 57	42, 44	6, 19	9, 65
	39	70	38	56	40	62	30	37	71	60	48	72

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p-1 = 72$, $z_\delta =$ 5,11,13,14,15,20,26,28,29,31,33,34,39,40,42,44,45,47,53,58,59,60,62,68

$\delta = 36$, $z_\delta =$ 6,12,19,23,25,35,38,48,50,54,61,67

$\delta = 24$, $z_\delta =$ 7,17,21,30,43,52,56,66

$\delta = 18$, $z_\delta =$ 18,36,41,57,69,71

$\delta = 12$, $z_\delta =$ 3,24,49,70

$\delta = 9$, $z_\delta =$ 2, 4,16,32,37,55

$\delta = 8$, $z_\delta =$ 10,22,51,63

$\delta = 6$, $z_\delta =$ 9,65

$\delta = 4$, $z_\delta =$ 27,46

$\delta = 3$, $z_\delta =$ 8,64

$\delta = 2$, $z_\delta =$ 72

$\delta = 1$, $z_\delta =$ 1

$\boxed{p = 79} = 4n-1$

$$z^2 = \mathfrak{G}p + r$$

r =	1	2	4	5	8	9	10	11	13	16	18	19	20	21	22	23	25	26	31	32	36
z =	1	9	2	20	18	3	22	13	31	4	27	16	39	10	38	24	5	37	30	36	6
	78	70	77	59	61	76	57	66	48	75	52	63	40	69	41	55	74	42	49	43	73

r =	38	40	42	44	45	46	49	50	51	52	55	62	64	65	67	72	73	76
z =	14	35	11	26	19	21	7	34	29	17	23	33	8	12	15	25	28	32
	65	44	68	53	60	58	72	45	50	62	56	46	71	67	64	54	51	47

$$z^{3} = \mathfrak{G}p + r$$

falsch z^3

r =	1	8	10	12	14	15	17	18	21	22	27	33	38
z =	1, 23	2, 31	40, 51	27, 63	37, 60	17, 66	47, 54	9, 21	20, 65	44, 50	3, 7	41, 43	8, 26
	55	46	67	68	61	75	57	49	73	64	69	74	45

r =	41	46	52	57	58	61	62	64	65	67	69	71	78
z =	34, 53	5, 36	10, 72	15, 29	6, 14	30, 58	22, 25	4, 13	18, 19	11, 16	12, 28	33, 48	24, 56
	71	38	76	35	59	70	32	62	42	52	39	77	78

$$z^{13} = \mathfrak{G}p + r$$

r =	1	23	24	55	56	78
z =	1,8,10,18,21,22,38	4,5,9,11,19,23,26	3,24,28,30,34,35,37	2,13,16,20,25,36,42	6,7,29,39,47,48,53	12,14,15,17,27,33,41
	46,52,62,64,65,67	31,32,40,50,72,73	43,54,59,63,66,77	44,45,49,51,55,76	56,60,68,70,74,75	57,58,61,69,71,78

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p-1 = 78$, $z_\delta =$ 3, 6, 7,28,29,30,34,35,37,39,43,47,48,53,54,59,60,63,66,68,70,74,75,77

$\delta = 39$, $z_\delta =$ 2, 4, 5, 9,11,13,16,19,20,25,26,31,32,36,40,42,44,45,49,50,51,72,73,76

$\delta = 26$, $z_\delta =$ 12,14,15,17,27,33,41,57,58,61,69,71

$\delta = 13$, $z_\delta =$ 8,10,18,21,22,38,46,52,62,64,65,67

$\delta = 6$, $z_\delta =$ 24,56

$\delta = 3$, $z_\delta =$ 23,55

$\delta = 2$, $z_\delta =$ 78

$\delta = 1$, $z_\delta =$ 1

$\boxed{p = 83} = 4n - 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1	3	4	7	9	10	11	12	16	17	21	23	25	26	27	28	29	30	31	33	36
$z =$	1	13	2	16	3	33	29	26	4	10	41	40	5	21	39	32	19	14	23	38	6
	82	70	81	67	80	50	54	57	79	73	42	43	78	62	44	51	64	69	60	45	77

$r =$	37	38	40	41	44	48	49	51	59	61	63	64	65	68	69	70	75	77	78	81
$z =$	28	11	17	37	25	31	7	36	15	12	35	8	27	20	22	30	18	34	24	9
	55	72	66	46	58	52	76	47	68	71	48	75	56	63	61	53	65	49	59	74

$$z^{41} = \mathfrak{G}p + r$$

$r =$	1,	82
$z =$	1,3,4,7,9,10,11,12,16,17,21,23,25,26,27,28,29,30,31,33,36,37 38,40,41,44,48,49,51,59,61,63,64,65,68,69,70,75,77,78,81	2,5,6,8,13,14,15,18,19,20,22,24,32,34,35,39,42,43,45,46,47,50 52,53,54,55,56,57,58,60,62,66,67,71,72,73,74,76,79,80,82

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p-1 = 82,\quad z_\delta = 2,5,6,8,13,14,15,18,19,20,22,24,32,34,35,39,42,43,45,46,47,50,52,53,$
$54,55,56,57,58,60,62,66,67,71,72,73,74,76,79,80$

$\delta = 41,\quad z_\delta = 3,4,7,9,10,11,12,16,17,21,23,25,26,27,28,29,30,31,33,36,37,38,40,41,$
$44,48,49,51,59,61,63,64,65,68,69,70,75,77,78,81$

$\delta = 2,\quad z_\delta = 82$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 89} = 4n + 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1	2	4	5	8	9	10	11	16	17	18	20	21	22	25	32	34	36	39	40	42	44
$z =$	1	25	2	19	39	3	30	10	4	27	14	38	33	17	5	11	37	6	22	29	24	20
	88	64	87	70	50	86	59	79	85	62	75	51	56	72	84	78	52	83	67	60	65	69

$r =$	45	47	49	50	53	55	57	64	67	68	69	71	72	73	78	79	80	81	84	85	87	88
$z =$	32	15	7	36	26	12	18	8	44	35	43	31	28	42	16	41	13	9	23	21	40	34
	57	74	82	53	63	77	71	81	45	54	46	58	61	47	73	48	76	80	66	68	49	55

$$z^{11} = \mathfrak{G}p + r$$

$r =$	1,	12,	34,	37,	52,	55,	77,	88
$z =$	1, 2, 4, 8 16,32,39,45 64,67,78	19, 27, 29, 37 38, 54, 58, 59 63, 74, 76	9, 18, 21, 36 42,49,55,69 72, 79, 84	3, 6, 7, 12 14,23,24,28 46, 48, 56	33, 41, 43, 61 65, 66, 75, 77 82, 83, 86	5, 10, 17, 20 34,40,47,53 68, 71, 80	13, 15, 26, 30 31, 35, 51, 52 60, 62, 70	11, 22, 25, 44 50, 57, 73, 81 85, 87, 88

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p-1 = 88,\quad z_\delta = 3,6,7,13,14,15,19,23,24,26,27,28,29,30,31,33,35,38,41,43,46,48,51,54,$
$56,58,59,60,61,62,63,65,66,70,74,75,76,82,83,86$

$\delta = 44,\quad z_\delta = 5,9,10,17,18,20,21,36,40,42,47,49,53,68,69,71,72,79,80,84$

$\delta = 22,\quad z_\delta = 11,22,25,44,50,57,73,81,85,87$

$\delta = 11,\quad z_\delta = 2,4,8,16,32,39,45,64,67,78$

$\delta = 8,\quad z_\delta = 12,37,52,77$

$\delta = 4,\quad z_\delta = 34,55$

$\delta = 2,\quad z_\delta = 88$

$\delta = 1,\quad z_\delta = 1$

$\boxed{p = 97} = 4n + 1$

$$z^2 = \mathfrak{G}p + r$$

$r =$	1	2	3	4	6	8	9	11	12	16	18	22	24	25	27	31	32	33	35	36	43	44	47	48
$z =$	1	14	10	2	43	28	3	37	20	4	42	33	11	5	30	15	41	18	36	6	25	23	12	40
	96	83	87	95	54	69	94	60	77	93	55	64	86	92	67	82	56	79	61	91	72	74	85	57
$r =$	49	50	53	54	61	62	64	65	66	70	72	73	75	79	81	85	86	88	89	91	93	94	95	96
$z =$	7	27	21	32	35	16	8	29	39	19	13	48	47	46	9	45	38	31	34	24	44	26	17	22
	90	70	76	65	62	81	89	68	58	78	84	49	50	51	88	52	59	66	63	73	53	71	80	75

$$z^3 = \mathfrak{G}p + r$$

$r =$	1	8	12	18	19	20	22	27	28	30	33	34	42	45	46	47
$z =$	1, 35	2, 25	18, 31	44, 65	26, 34	55, 57	6, 16	3, 8	5, 14	10, 28	47, 54	30, 80	23, 29	46, 58	20, 21	33, 73
	61	70	48	85	37	82	75	86	78	59	93	84	45	90	56	88
$r =$	50	51	52	55	63	64	67	69	70	75	77	78	79	85	89	96
$z =$	9, 24	41, 76	7, 39	52, 68	13, 17	4, 43	38, 69	19, 83	11, 89	22, 81	15, 40	60, 63	12, 32	49, 66	27, 72	36, 62
	64	77	51	74	67	50	87	92	94	91	42	71	53	79	95	96

$$z_\delta^\delta = \mathfrak{G}p + 1$$

$\delta = p - 1 = 96$, $z_\delta =$ 5, 7,10,13,14,15,17,21,23,26,29,37,38,39,40,41,56,57,58,59,60,68, 71,74,76,80,82,83,84,87,90,92

$\delta = 48$, $z_\delta =$ 2, 3,11,25,31,32,44,48,49,53,65,66,72,86,94,95

$\delta = 32$, $z_\delta =$ 19,20,28,30,34,42,45,46,51,52,55,63,67,69,77,78

$\delta = 24$, $z_\delta =$ 4, 9,24,43,54,73,88,93

$\delta = 16$, $z_\delta =$ 8,12,18,27,70,79,85,89

$\delta = 12$, $z_\delta =$ 6,16,81,91

$\delta = 8$, $z_\delta =$ 33,47,50,64

$\delta = 6$, $z_\delta =$ 36,62

$\delta = 4$, $z_\delta =$ 22,75

$\delta = 3$, $z_\delta =$ 35,61

$\delta = 2$, $z_\delta =$ 96

$\delta = 1$, $z_\delta =$ 1

$$\boxed{p = 101} = 4n+1$$

$$z^2 = \mathfrak{S}p + r$$

$r =$	1	4	5	6	9	13	14	16	17	19	20	21	22	23	24	25	30
$z =$	1, 100	2, 99	45, 56	39, 62	3, 98	35, 66	32, 69	4, 97	44, 57	25, 76	11, 90	18, 83	27, 74	15, 86	23, 78	5, 96	38, 63
$r =$	31	33	36	37	43	45	47	49	52	54	56	58	64	65	68	70	71
$z =$	43, 58	29, 72	6, 95	21, 80	12, 89	34, 67	42, 59	7, 94	31, 70	16, 85	37, 64	19, 82	8, 93	41, 60	13, 88	26, 75	24, 77
$r =$	76	77	78	79	80	81	82	84	85	87	88	92	95	96	97	100	
$z =$	50, 51	28, 73	49, 52	33, 68	22, 79	9, 92	48, 53	36, 65	40, 61	17, 84	47, 54	30, 71	14, 87	46, 55	20, 81	10, 91	

$$z^5 = \mathfrak{S}p + r$$

$r =$	1	6	10	14	17	32	36	39	41	44
$z =$	1, 36, 84, 87, 95	22, 30, 70, 85, 96	10, 32, 41, 57, 62	4, 33, 43, 45, 77	13, 20, 23, 64, 82	2, 67, 72, 73, 89	25, 52, 54, 80, 92	26, 27, 40, 46, 63	3, 7, 50, 59, 83	8, 53, 66, 86, 90
$r =$	57	60	62	65	69	84	87	91	95	100
$z =$	11, 15, 35, 48, 93	18, 42, 51, 94, 98	38, 55, 61, 74, 75	9, 21, 47, 49, 76	12, 28, 29, 34, 99	19, 37, 78, 81, 88	24, 56, 58, 68, 97	39, 44, 60, 69, 91	5, 16, 31, 71, 79	6, 14, 17, 65, 100

$$z_\delta^\delta = \mathfrak{S}p + 1$$

$\delta = p-1 = 100$, $z_\delta =$ 2, 3, 7, 8,11,12,15,18,26,27,28,29,34,35,38,40,42,46,48,50,51,53,
55,59,61,63,66,67,72,73,74,75,83,86,89,90,93,94,98,99

$\delta = 50$, $z_\delta =$ 4, 9,13,20,21,22,23,30,33,43,45,47,49,64,70,76,77,82,85,96

$\delta = 25$, $z_\delta =$ 5,16,19,24,25,31,37,52,54,56,58,68,71,78,79,80,81,88,92,97

$\delta = 20$, $z_\delta =$ 32,39,41,44,57,60,62,69

$\delta = 10$, $z_\delta =$ 6,14,17,65

$\delta = 5$, $z_\delta =$ 36,84,87,95

$\delta = 4$, $z_\delta =$ 10,91

$\delta = 2$, $z_\delta =$ 100

$\delta = 1$, $z_\delta =$ 1

Tafel III.

Die Zahlen	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	5	5	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	7	.	7	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	11	.	.	.	11	11	11	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	13	.	.	.	13	13	.	.	.	13	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	17	.	17	17	17	.	.	17	17	17	.	17	.	.	.	.	.	.	.	.	.	.	.	.
	19	19	.	.	.	.	.	.	19	.	.	19	19	19	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	23	.	23	.	.	23	23	.	.	23	23	.	23	.	23	23	23	.	.	.	.	.
	29	29	.	.	.	.	29	.	29	29	.	.	29	29	.	.	29	29	.	29	.	.	.	.	29
	.	31	.	.	.	.	.	.	.	31	31	31	.	.	.	31	.	.	.	31	31	.	31	.	.
	37	.	.	37	.	.	.	.	.	.	.	37	.	37	.	37	37	37	37	.	37	.	37	.	.
sind Haupt-stammwurzeln zu	.	.	.	.	41	41	.	.	.	41	41	41	.	41	.	41	.	41	.	.	41	.	41	.	41
	.	43	.	43	.	.	.	.	.	.	43	.	.	.	.	.	43	43	43	.	.	.	.	.	43
	.	.	.	47	.	.	.	.	47	47	.	47	.	47	.	.	.	47	47	.	47	47	.	.	47
	53	53	.	53	.	.	53	.	.	.	53	.	53	.	.	.	53	53	53	53	53	.	.	.	53
	59	.	.	.	59	.	59	.	59	59	.	59	59	.	.	.	59	.	.	.	.	59	59	.	.
	61	.	.	.	61	61	.	.	61	.	.	.	.	.	.	61	61	.	.	.	.	.	.	.	61
	67	.	.	.	.	67	.	.	.	67	67	67	.	.	.	.	67	.	67	.	.	.	.	.	.
	.	.	.	73	.	.	.	.	.	73	.	73	73	73	.	.	.	.	73	.	.	.	.	.	73
	.	79	.	.	79	79	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	83	.	.	83	83	.	83	.	.	.	.	83	83	83	.	.	83	83	83	.	83	.	83	.	.
	.	89	.	.	89	89	.	.	.	.	.	89	89	89	.	.	.	89	.	.	.	89	89	.	89
	.	.	.	97	.	97	.	.	97	.	.	97	97	97	.	97	.	.	.	97	.	97	.	.	97
	101	101	.	.	.	101	.	.	.	101	101	.	.	101	.	.	101	.	.	.	.	.	.	.	101

Die Zahlen	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	29	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	37	.	.	37	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
sind Haupt-stammwurzeln zu	.	41	41	41	.	.	.	41	41	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	43	43	43	.	.	43	43	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	47	47	47	.	47	.	47	.	.	47	47	47	47	.	47	47	47	.	.	.	.	.
	53	.	.	.	53	53	53	53	53	.	.	.	53	.	53	.	.	.	53	.	.	53	.	53
	.	.	.	59	59	59	59	59	.	.	59	59	59	59	.	59	59	59	.	.	59	.	.	59
	.	.	.	61	61	.	.	.	61	.	.	.	.	.	.	.	61	61	.	.	.	.	.	.
	.	67	.	.	67	67	.	67	.	.	.	.	.	.	67	.	.	67	.	67	.	67	.	67
	.	73	73	.	73	.	73	73	.	.	.	.	73	73	.	73	.	73	73	.	73	.	.	.
	.	79	79	79	.	.	.	79	79	.	79	.	79	.	.	79	.	.	.	.	79	79	.	.
	.	.	.	.	.	83	.	83	83	.	.	.	83	.	.	83	83	.	83	83	83	.	.	83
	89	89	89	89	89	.	89	.	89	.	.	89	.	.	89	.	89	.	.	89	.	89	.	.
	.	.	97	.	.	.	.	.	.	.	97	97	97	97	97	.	.	.	.	.	.	.	.	.
	101	101	101	.	.	.	.	101	101	.	.	101	.	101	.	101	.	.	.	101	.	101	.	101

Die Zahlen	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
	53	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	59	.	59	59	59	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	61	.	.	61	61	.	61	.	61	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	67	.	.	.	.	.	.	.	.	.	67	.	67	.	.	.	.	.	.	.	.	.	.	.	.
sind Haupt-stammwurzeln zu	.	.	73	.	.	.	.	73	73	73	.	73	.	.	.	.	.	73	.	.	.	.	.	.	.
	.	.	79	79	.	.	.	.	79	79	.	.	79	.	.	79	.	79	.	79	.	.	.	79	79
	.	83	83	83	83	83	83	83	.	83	.	83	.	.	83	83	83	.	.	.	83	83	83	83	.
	89	.	.	89	.	89	.	89	89	89	89	89	89	.	.	89	.	.	.	89	.	.	.	89	89
	.	.	.	.	.	97	97	97	97	97	.	.	.	.	.	.	.	97	.	.	97	.	.	97	.
	101	.	101	.	101	.	.	.	101	.	101	.	101	.	.	101	101	.	.	.	.	101	101	101	101

Die Zahlen	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
sind Haupt-stammwurzeln zu	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	79	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	83	.	.	83	83	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	89	.	.	.	.	.	89	89	.	.	89	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	97	.	.	.	97	.	97	97	97	.	.	97	.	.	97	.	97	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	101	.	.	101	.	.	101	101	.	.	101	101	.	.	.	101	101	.

Fremd

Bayerische StaatsBibliothek
Münchener DigitalisierungsZentrum Digitale Bibliothek

Crelle, August L.,

Encyklopädische Darstellung der Theorie der Zahlen und einiger anderer damit in Verbindung stehender analytischer Gegenstände zur Beförderung und allgemeineren Verbreitung des Studiums der Zahlenlehre durch den ö ffentlichen und Selbst-Unterricht
Bd.: 1

Berlin (1845)

4 Math.u. 16 l-1
urn:nbn:de:bvb:12-bsb10525454-6